G00219366

Magic Quadrant for SSL VPNs

Published: 12 December 2011

Analyst(s): John Girard

Secure Sockets Layer virtual private networks compose a mature market segment, serving a variety of VPN use cases for workstations and mobile-device remote access.

What You Need to Know

Remote access is a fact of everyday life for IT-enabled employees who work with a mixture of business-provided and personally owned devices that are increasingly in continuous contact with the Internet. The solution space for remote-access VPNs includes many protocols, but the most significant are: (1) IPsec, a long-used protocol implemented as a Layer 3 tunnel; and (2) Secure Sockets Layer (SSL), which can be used to establish Layer 7 application sessions, as well as Layer 3 tunnels. Secure Shell (SSH) is occasionally implemented along with or in ways complementary to SSL. SSL VPN products all support an updated protocol — Transport Layer Security (TLS) — that provides Advanced Encryption Standard (AES) encryption, but "SSL" persists as the official label.

Multimodal remote access creates a need for vigilant security that works across multiple devices and OSs, taking the working definition of a remote-access VPN well beyond the basic need for an encrypted transport connection. Gartner has tracked the SSL VPN market for approximately 10 years, during which time SSL remote-access products and services have established a long-term role in business access. During this period, SSL has been the most disruptive force in VPNs because of its versatility in providing encrypted access from nearly any computing device, combined with reverse-proxy isolation, menu-driven and clientless front ends, and several forms of network access controls designed to verify client system health and to quarantine sensitive information.

Gartner ranks vendors in the SSL VPN Magic Quadrant based on performance for the four quarters of 2010 through the end of September 2011, and on client reviews received up to November 2011. The Magic Quadrant considers which vendors will be in frequent use and will influence technology directions through 2016, as well as which vendors are the most visible among clients, generate the greatest number of requests for information and contract reviews, and account for the most new and ongoing installations among Gartner's client base.

After reading this Magic Quadrant, VPN planners will gain an understanding of the role of SSL VPNs in remote access and will be prepared to evaluate the suitability of SSL VPNs in company remote-access use cases. VPN planners should use the Magic Quadrant analysis comments to understand competitive differentiations between product and service offerings. All the vendors that Gartner tracks in the SSL VPN market have products that will meet the needs of most buyers. SSL VPNs are practical to complement or replace IPsec VPNs. They are easy to set up in their default role as application portals, and offer good performance for tunneled Layer 3 traffic, if desired. SSL VPN's resilience over poor connections and ability to conduct dynamic endpoint security checks has strong appeal for when access from noncompany devices must be controlled, including use cases for contractors and business continuity.

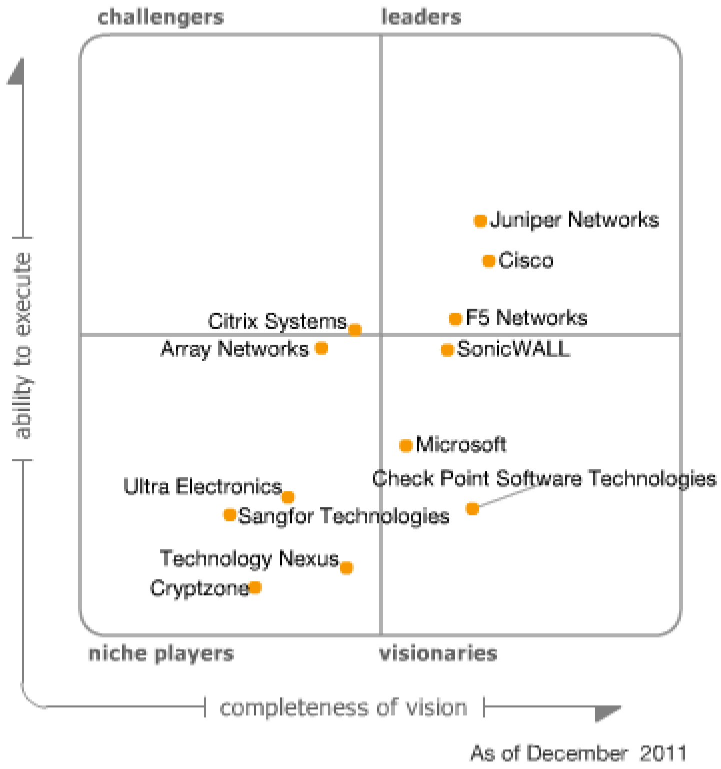
Gartner offers a Toolkit with suggested questions for an RFI/RFP evaluation of SSL VPNs (see "Toolkit: Secure Sockets Layer Virtual Private Network RFI and RFP Templates"). After considering this report and conducting their own RFI/RFP surveys, VPN planners should apply their findings to the following decision steps:

- Consider your incumbent networking and application delivery vendors, which may also provide VPN products and services. There are benefits for avoiding additional contracts, consoles and training. Where applicable, consider vendor ratings, strengths and challenges in adjacent markets — such as WAN optimization, application delivery, Web conferencing, Web access management (WAM) and enterprise single sign-on (ESSO).
- Demand a comprehensive working demonstration in the RFP phase. SSL VPNs are easy to set up. Make the vendors prove their worth, and you might even get the first prototype of your eventual production system for free. Be sure to ask for demonstrations for smartphone and tablet support, even if these are not part of your immediate VPN plan.
- Consider the ease of setup and administration, on-demand security, granular access policies, and other features that characterize products in this market. These aspects will lower the cost of ownership — even if your initial purchase is more expensive than a basic IPsec VPN.

Based on market dynamics, Gartner will discontinue the SSL VPN Magic Quadrant after this 2011 report. In 2012, SSL VPN will become a mature VPN capability that will primarily be sold as part of larger network infrastructure decisions rather than as stand-alone investments, although SSL VPNs may be delivered as stand-alone servers in the larger infrastructure for scalability and reliability purposes. In many cases, SSL VPNs will be integrated with next-generation firewalls and unified threat management (UTM) solutions.

Magic Quadrant

Figure 1. Magic Quadrant for SSL VPNs



Source: Gartner (December 2011)

Market Overview

SSL VPNs are persistent encrypted connections between user systems and VPN gateways, using the SSL protocol. SSL was originally conceived to intermittently secure protocol Layer 7 for browser sessions, but it has expanded to provide a broader range of access, ranging from Layer 7 for applications, down to Layer 3 for access to networks. SSL VPNs have been evaluated in a Magic Quadrant, because for many years, they were the focal point for innovations in remote access. SSL VPN technology has been a good source of revenue for network infrastructure companies, large and small, for more than 10 years. Industry revenues and shipments of SSL technologies are trackable and have met Gartner's criteria for defining and tracking a technology market. Most importantly, clients cite SSL and browser-based VPNs as key decision factors in new and upgraded VPN investments.

SSL VPNs are best characterized by the fact that the user can start a VPN session from a Web browser, although nearly all vendors offer a non-browser-client alternative. SSL VPN gateways feature a menu-driven, embedded reverse-proxy front end to provide a default greeting screen to a remote user, which can be dynamically configured according to access policies and contexts. The menu and resources offered to the user can be altered by runtime rules that react to the user's access status with respect to a variety of factors, including remote-system health security status, and the user's method of authentication. SSL's advantages for VPNs include:

- The VPN can be established without a formally installed client beyond the browser, and supports the mainstream standard for encryption strength.
- SSL sessions can survive unreliable networks and multiple interruptions, and can reconnect and roam across networks without preserving an IP address.
- Nonbrowser SSL VPN clients increase the user's experience of transparency, while providing SSL reliability benefits. They can also support location-independent, IP-address-independent "connect on demand" situations, which are particularly attractive on small mobile devices with limited battery life.
- SSL VPNs feature security tools that can be downloaded to end-user systems during session establishment. These tools enhance network access control (NAC) decisions by performing client-side health checks, even on systems that have never before made a VPN connection. User references obtained for this year's Magic Quadrant report indicate increased utilization of these tools.

SSL VPNs shield the user from the LAN by default, and Layer 3 tunnels to support routing can be limited by policy choices. These policies can be set dynamically, based on gateway rules that evaluate the user, device and location. When users initiate a VPN from an unmanaged device, remote security controls may not be possible, but administrators can use SSL VPNs to mitigate the risk of network exposures by limiting applications and services.

Compelling use cases for SSL VPNs include:

- They provide selective access to systems on a need-to-know basis, allowing relatively easy access partitioning to support use cases, such as contractors, personal employee devices and ad hoc emergency access from unknown systems.
- They provide secure intranet or Internet business portals. SSL VPNs, combined with Web-enabled business applications, create instant, robust portals capable of extending strong authentication and health checks.
- They provide ad hoc private service to support unplanned and emergency remote-access needs.

Limiting factors for SSL VPNs include:

- IPsec is deeply embedded in networking products, such as routers and firewalls, and has a lower incremental session cost in gateways. SSL VPNs have historically represented an extra cost.
- Many companies are satisfied with their IPsec experiences. If the legacy VPN meets business needs, there is no pressure to change.

- The major mobile-device OSs include mobile IPsec clients. IPsec is easy to configure on some mobile devices, such as iPhones and iPads, and can support connection on-demand, which conserves battery life. Also, several specialized legacy mobile VPNs have success records relying neither on SSL nor IPsec.

Twelve vendors returned survey data for this Magic Quadrant. The selection of vendors includes all geographies, with the greatest emphasis evenly averaged between North America, Europe and Asia/Pacific. Among the vendors that provided data for this Magic Quadrant, the comparative year-over-year growth of revenue within each vendor's SSL VPN line of business (LOB) was positive. Reported and estimated revenue for the LOB containing SSL VPN (which may include related products, as well as support and services) totaled about $443 million, increasing from $400 million last year. This amounts to an 11% increase that is slightly better than Gartner's growth forecast across a larger selection of vendors selling specialized SSL VPN equipment worldwide, reported at a 9% compound annual growth rate (CAGR) through 2015 (see "Forecast: Specialized SSL VPN Equipment, Worldwide, 2005-2015, 4Q11 Update").

This rate of growth is sufficient to justify SSL technology as a valued component in the infrastructure of incumbent vendors but is not enough to suggest that SSL VPN will continue to drive a differentiated VPN market (see "Forecast: Specialized SSL VPN Equipment, Worldwide, 2005-2015, 4Q11 Update"). Vendors surveyed for this Magic Quadrant reported individual growth for the LOB containing SSL VPN that ranged from 2% to 44% over the previous year. Our 2011 assessment of the SSL VPN market remains cautious. SSL technology has proven, long-term viability as a tool in the kit of network and security planners. However, as a stand-alone market, SSL VPN is showing its age.

Seat sales (seat sessions or penetrations) are estimated for this Magic Quadrant to be usable concurrent VPN sessions on product gateways. Vendors that do not set maximum capacity limits on their products were asked to estimate the number of ports available on products sold, according to the recommended loading. The number obtained represents the usable logical sessions in play.

Seat penetrations, calculated based on results from 11 vendors reporting seat data (Citrix Systems declined to participate in the survey), add up to a total of more than 18 million for full-year 2010, an 80% increase compared with 10 million recorded in the study period of the previous Magic Quadrant. In previous Magic Quadrant reports, the performance of reporting vendors increased only 32% from 2008 to 2009 in a difficult economy. We attribute much of this growth to an improved economy, increasing numbers of teleworkers (particularly in government positions), increasing interest in business continuity program development, and spare capacity purchase decisions.

Based on a full-year 2010 analysis, the reporting vendors generated average seat penetrations of 2 million seats, up from 940,000 in 2009. The median share also increased to 358,000 seats, compared with 250,000 in the prior year, which had in fact been a 25% slump from 2008. At the same time, median income in the SSL VPN LOB increased to about $18.7 million, up from $15 million, but this is still a slump from $19.5 million in 2008. The 2011 economy appears favorable to all of the tracked vendors, and their estimates for 2011 full-year performance are on track for healthy improvements in sales revenue and seat penetrations that will exceed those of the prior year.

Market Definition/Description

Products in the SSL VPN market provide secure and private connections for individuals to reach company gateways via the Internet using the SSL protocol from a workstation, such as a desktop, laptop, or a smaller end-user computing device, such as a smartphone or tablet. This Magic Quadrant evaluates SSL VPN products that are sold for purchase and use within enterprises.

SSL VPN products combine browser security enhancement software with a VPN gateway that may be delivered as a stand-alone gateway appliance or as software to be installed on a user-supplied gateway server. The market is dominated by appliances; however, pure software products are becoming more popular through virtualization, which makes it easy to develop drop-in, scalable, plug-and-play solutions for gateway production systems, as well as to evaluate presale demonstrations. Menu-driven, "point and click" browser access to programs and resources characterize the default interface for an SSL VPN; however, several companies offer nonbrowser clients to more closely imitate an IPsec VPN, and a few companies omit the menu interface altogether.

SSL VPNs support the strong authentication and session logging desired for VPN protection, as well as application access audits. They also support the roaming requirements for mobile users, especially those carrying notebook computers and, increasingly, smartphones and tablets. The most commonly requested mobile support in 2011 has been for iPhones and iPads, making Apple devices an important point for competitive differentiation.

Inclusion and Exclusion Criteria

Inclusion Criteria

SSL VPN companies were considered for this Magic Quadrant under the conditions listed here. We contacted 26 companies, and 12 were qualified to be ranked:

- The company must sell a VPN product that fits the SSL VPN market definition, and is commercially supported.
- The vendor must generate sufficient Gartner client interest and inquiries, especially by evidence of their appearance in shortlists and RFIs.
- The vendor should appear regularly in other sources, such as publications, support forums and conferences, as a product that is competitive with companies that are qualified for this market.
- The vendor must demonstrate competitive presence and sales to Gartner analysts. Competitive presence is improved greatly if the product is sold and supported in multiple countries — or, even better, in multiple geographies. Exceptions may be granted if other inclusion factors merit consideration. Gartner analysts evaluate feedback from clients who contact analysts for inquiries, as well as from nonclients, including referrals of users provided by vendors during the survey process.
- For 2011, minimum thresholds for seat sales and revenue have been continued. To qualify for inclusion, vendors had to meet both of these conditions:

- A qualifying vendor needed to earn at least $1 million in revenue in 2010 in the worldwide LOB for SSL VPNs. In this Magic Quadrant, no ranked vendor earned less than $4.5 million. Many of the vendors in this Magic Quadrant are small companies, or large companies with small earnings in this market.
- A qualifying vendor needed to account for at least 100,000 cumulative concurrent user/seat sessions in play for 2008, 2009 and 2010. In this Magic Quadrant, no ranked vendor reported fewer than 200,000.

Exclusion Criteria

VPN companies have been excluded from the 2011 Magic Quadrant for one or more of these conditions:

- The company did not have a competitive product on the market for a sufficient amount of time during 2010 and the first half of 2011 to establish a visible, competitive position and track record.
- The company had a minimal or negligible apparent market share and market inquiry interest among Gartner clients.
- The company sells the product primarily as an application firewall or other specialized interface that is not competing directly within the larger SSL VPN product or function.
- The company sells Web-enabled, personal remote-control products that are not true multiuser access gateways.
- The company was invited to participate, but did not reply to an annual RFI and did not otherwise meet the inclusion criteria. Alternative means of assessment, particularly client requests and competitive visibility, did not meet the inclusion criteria.
- Services built from the products and offered by third parties are considered additive to the product vendor's ranking, and the service vendors are not ranked. Managed network services of all types are separate markets.
- Due to changes in internal direction or acquisition, a previously ranked company no longer operates in a directly competitive stance for the SSL VPN market.

Other Companies

Companies that have products in the market but are not ranked in this report include Avaya, Barracuda Networks, Elitecore Technologies (Cyberoam), HOB GmbH, Fortinet, Lantronix, O2Security, Palo Alto Networks, Stonesoft and WatchGuard Technologies.

Added

- Cryptzone acquired AppGate and is added to this report.
- Technology Nexus has acquired PortWise and is added to this report.

- Ultra Electronics acquired AEP Networks and is added to this report.

Dropped

- AEP Networks has been acquired by Ultra Electronics and is now ranked under the name Ultra Electronics.
- AppGate was acquired by Cryptzone and is now ranked under the name Cryptzone.
- NeoAccel was acquired by VMware to add network privacy capabilities into the company's product lines for security, VMware View and cloud, versus directly competing for a stand-alone VPN market share. VMware has declared the end of life for the stand-alone NeoAccel appliance, and will pursue new virtual technology developments in which NeoAccel will provide new enabling technologies for remote access.
- PortWise has been integrated into a new company called Technology Nexus and is ranked under that name.

Evaluation Criteria

Ability to Execute

Execution considers factors related to getting products sold, installed, supported and in user hands. Companies that execute strongly generate pervasive awareness and loyalty among Gartner clients, as well as a steady stream of inquiries to Gartner analysts. Execution is not primarily about company size and income; however, as the market matures, larger companies tend to have a greater influence on the market. We track influence on buyers through revenue and seat sales. We track influence among vendors in the market through client feedback about shortlist decisions, as well as on comments from each vendor about its peer group, including perceived threats and competitive self-assessment. For three years running, Juniper Networks, Cisco and Citrix Systems were voted by their peers as the most serious competitive threats in the market.

New products, new features and estimated sales in 1H11 were considered in the final ranking. Unofficial road maps, pending contracts, future sales agreements, future promises for very recent acquisitions and vague strategies do not significantly contribute to a vendor ranking or to inclusion in this Magic Quadrant; however, vendors that have official and public road maps, and make consistent progress, are recognized.

Execution weightings are considered standard, because within our review, the relative merit of each ranking factor can be adequately expressed for the general case without additional adjustments. Weightings are subjective and contextual; readers who conduct their own RFIs may choose to change weightings to suit the needs of their business and their industry. Weighting suggestions and detailed survey questions are presented in "Toolkit: Secure Sockets Layer Virtual Private Network RFI and RFP Templates." Following are descriptions of the evaluation criteria for execution:

- **Product/Service:** Compares the completeness and appropriateness of core SSL VPN products sold for use in the enterprise remote-access market. The SSL VPN market defined in this Magic Quadrant is product-focused, but related service areas may contribute, including consulting services and managed service resellers. A strong product focus is critical to demonstrating that the vendor can generate market awareness.

- **Overall Viability (Business Unit, Financial, Strategy, Organization):** Considers the company's history and its demonstrated commitment in the SSL VPN market, as well as the difference between a company's stated goals for the evaluation period and actual performance, as compared with the rest of the market. The growth of the customer base and the revenue derived from sales are considered. All vendors were asked to disclose comparable market data, such as SSL VPN revenue, the number of unique companies under contract and information about seats sold year by year. "Seats" are defined as concurrent active license seats deployed on sold products. Where companies have moved to an unlimited-license model, active seats are estimated from the normal capacity limits of the platforms sold.

  Some vendors do not report portions of competitive information in the format requested for comparison. In these situations, other quantitative sources of Gartner information were considered, but qualitative evidence from client feedback and peer analyst feedback become more important. Indirect measures of product penetration, such as "boxes shipped," were not used to measure execution in this Magic Quadrant. Instead, we considered concurrent seats sold, licensed and accessible to the buyer as evidence that the products are being used. Vendors were asked to convert to the concurrent seat formula as necessary, and the actual numbers reported were treated as guidance, rather than as hard facts.

- **Sales Execution/Pricing:** Compares the strength of vendors' sales and distribution operations, as well as their discounted list pricing for systems supporting as few as 25 concurrent users and up to more than 10,000 concurrent users. Pricing was compared in first-year, cost-per-concurrent-active-license seats, including the cost of all hardware and support.

- **Market Responsiveness and Track Record, and Marketing Execution:** Rates competitive visibility as the key factor, including which vendors are most commonly considered the top competitive threats during the RFP process and which are considered the top threats by peers. In addition to buyer and analyst feedback, this rating considers feedback from clients, analysts and the vendors themselves. Strong ratings mean that a company has demonstrated to Gartner analysts that the enterprise can get listed in RFPs early and can win a large percentage in competition with other vendors. Marketing execution in this Magic Quadrant is considered an aspect of market responsiveness and track record, rather than a separate criterion.

- **Customer Experience:** Is subjectively rated from client feedback to analysts; the opinions of Gartner analysts in security, network and platform research groups; and vendor-supplied references, where needed. Intense interest in SSL VPNs from Gartner clients provided a year's worth of ample feedback to frame the market.

- **Operations:** Considers the ability of a vendor to pursue goals in a manner that enhances and grows its influence in all execution categories.

Table 1 provides an overview of the evaluation criteria for the Ability to Execute.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	Standard
Overall Viability (Business Unit, Financial, Strategy, Organization)	Standard
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	Standard
Marketing Execution	No rating
Customer Experience	Standard
Operations	Standard

Source: Gartner (December 2011)

Completeness of Vision

The SSL VPN market is mature in terms of its core definition, and most vendors have functions and features that make them more similar rather than distinguished among peers. For the past two years, many SSL VPN vendors — particularly the smaller vendors — concentrated on selling into safe situations, and their investments in disruptive vision-differentiating activities were limited. Some of the R&D projects that required a lot of effort, such as building out support for virtualization, are now considered status quo rather than matters of differentiation.

Vision weightings are considered standard, because, within our review, the relative merit of each ranking factor can be adequately expressed for the general case without additional adjustments. Weightings are subjective and contextual; readers who conduct their own RFIs may choose to change weightings to suit the needs of their businesses and their industries. Weighting suggestions and detailed survey questions are presented in "Toolkit: Secure Sockets Layer Virtual Private Network RFI and RFP Templates." Following are descriptions of the evaluation criteria for vision:

- **Market Understanding and Marketing Strategy:** Assesses through direct observation the degree to which a vendor's products, road maps and mission anticipate leading-edge thinking about buyer wants and needs. Gartner makes this assessment subjectively by several means, including interaction with vendors in briefings and by reading planning documents, marketing and sales literature, and press releases. Incumbent vendor market performance is reviewed year by year against specific recommendations that have been made to each vendor and against future trends identified in Gartner research. Vendors cannot merely state an aggressive future goal; they must put these plans in place, show that they are following the plans and modify the plans as market directions change.
- **Sales Strategy:** Examines vendors' strategies for communicating their product messages. This ranking factor is the bridge between marketing execution and product strategy.

- **Offering (Product) Strategy:** Is ranked through an examination of the breadth of functions, platform and OS support for the SSL client; the VPN gateway OS and features; and the investments made by the vendor to optimize and support applications accessed through the gateway. R&D investments are credited in this category.
- **Business Model:** Takes into account a vendor's underlying business objectives for its products and its ongoing ability to pursue R&D goals in a manner that enhances all vision categories.
- **Vertical/Industry Strategy:** Considers a vendor's ability to communicate a vision that appeals to specific industries and vertical markets.
- **Innovation:** Takes into consideration the degree to which vendors invest in core requirements for the successful use of their products. Criteria include a vendor's internal investments in value-added security tools and technology road maps, as well as external efforts to expand interoperability, alliances and partnerships with companies in related security markets. A vendor with a strong vision creates communities with other companies, and this, in turn, helps other companies, as well as buyers, view the SSL VPN vendor as a necessary component of larger business solutions.
- **Geographic Strategy:** Takes into account a vendor's strategy to direct its resources, skills, products and services in multiple geographies.

Table 2 gives an overview of the evaluation criteria for Completeness of Vision.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	Standard
Marketing Strategy	Standard
Sales Strategy	Standard
Offering (Product) Strategy	Standard
Business Model	Standard
Vertical/Industry Strategy	Standard
Innovation	Standard
Geographic Strategy	Standard

Source: Gartner (December 2011)

Leaders

Leaders demonstrate balanced progress, effort and clout in all execution and vision categories. Their actions raise the competitive bar for all products in the market, and they can change the course of the industry. To remain in the Leaders quadrant, vendors must excel in performance, scalability and protection, and must dominate in sales. However, a leading vendor is not a default choice for all buyers, and clients are warned not to assume that they should buy only from the Leaders quadrant. To stay on the right side of the chart, Leaders (and Visionaries) must follow courses that are competitively disruptive, and not only are ahead of the curve, but also offer features that remove significant roadblocks to vendor sales and buyer implementations. One example of a competitively disruptive activity might include delivering a superior smartphone client in terms of capability, user experience and user adoption that could significantly stimulate new smartphone VPN deployments.

Vendors that have pursued new technologies but have not changed the course of buyer decisions and implementations, and companies that add features to make their products more complete in comparison with the same features offered by other vendors, are not creating competitively disruptive situations.

In a mature VPN market, Leaders sell broad network infrastructure product families to buyers, as well as stand-alone VPNs. Buyers of Leader products include larger companies and/or projects that often stretch products in ways that uncover problems in scalability and maintainability. Quick response is essential. Larger investments in help and support operations contribute greatly to satisfaction.

Challengers

Challengers have attractive products that address the typical needs of the market, with strong sales and visibility that add up to higher execution than Niche Players. Challengers are good at winning contracts, but they do so by competing on a limited selection of functions or a limited selection of prospect buyers. They may be perceived as a threat by other vendors, but that threat will be primarily focused on a limited class of buyers, rather than the VPN market as a whole. Challengers are efficient and expedient choices for defined access problems. Many clients consider Challengers to be the conservative, safe alternative to Niche Players.

Visionaries

Visionaries invest in the leading-edge or "bleeding edge" features that will be significant in next-generation products, and will give buyers early access to improved security and management. Visionaries can affect the course of technological developments in the market, but they lack the execution influence to outmaneuver Challengers and Leaders. Buyers pick Visionaries for best-of-breed features, and for broader network infrastructure investments than Niche Players. Buyers may obtain more personal attention. Visionaries may take risks on potentially disruptive technologies (as described in the Leaders section), and often, they do this without the financial reserves of a Leader or Challenger. Buyers of Visionaries' products may base their selections on specific technology features and on participation in the vendor's road map plans.

Niche Players

Niche Players offer viable, dependable solutions that meet the typical needs of buyers and fare well when given a chance to compete in a product evaluation. Niche Players respond to market changes and new technologies, but they generally lack the clout to change the course of the market. Niche Players may serve conservative and risk-averse buyers more efficiently than Leaders. Clients tend to select Niche Players as stand-alone or point solutions for SSL VPN when stability and focus on a few important functions and features are more important than a wide and long road map. Niche Players may target clients that, for various reasons, prefer not to buy from larger network players. Buyers report that Niche Players tend to provide more personal attention to their needs. Buyers of these VPN products are generally happy and do not stretch the systems past the design parameters. They are unlikely to switch vendors, but they may represent limited upsell opportunities.

Vendor Strengths and Cautions

Array Networks

Founded in 2000, Array Networks sells entry-level through carrier-class equipment into a number of related markets, including application delivery controllers, load balancing and SSL acceleration. Buyers are most strongly interested in VPN alternatives to IPsec and, frequently, combine SSL VPN with DesktopDirect, Array's fully monitored Remote Desktop Protocol (RDP) remote-access switch that works as a companion to the SSL VPN. Federal Information Processing Standard (FIPS) 140-2 Level 2 and Level 3 add-in encryption cards are available.

Strengths

- Array has a competitive price/performance, green IT designs (high performance with reduced power and reduced network overhead), and scalability for large and demanding access needs, while also offering an affordable, low-end entry point.
- Array's 2010 revenue grew 19% over 2009, which is in line with the median growth reported by companies responding to the Magic Quadrant survey.
- High-end performance reaches 64,000 concurrent sessions in a single appliance.

Cautions

- Array's competitive visibility is among the lowest reported. Sales and client recognition are strongest in Asia/Pacific, particularly in China and India. A long-anticipated overhaul of marketing and communications is under way.
- Array has not yet delivered a virtual appliance gateway. This is a needed feature to reach parity in the market, which has proven competitive among peers.

Check Point Software Technologies

Check Point Software Technologies' SSL VPN was developed in-house starting in 2002, as an integral part of its VPN-1 family, and augmented with Zone Labs technology to provide integrated security tools. Today, Check Point sells SSL VPN in the Connectra appliance, as a software blade in its security gateway family, as a virtual appliance for ESX and as stand-alone software to run on several server platforms. Check Point sells in all geographies, but is strongest in Europe and the U.S., followed by Asia/Pacific. Buyers are most interested in alternatives to IPsec VPNs, extranet/contractor access and disaster management/business continuity access. Check Point's remote-access solutions are natively certified to Common Criteria (CC) Evaluation Assurance Level 4 (EAL4), and the R65 HFA-30 offers native FIPS 140-2 Level 2 certification.

Strengths

- Check Point's entry-level SSL VPN configuration includes integrated firewall, IPsec VPN and an intrusion prevention system (IPS). Other features of a UTM configuration are easily added as "software blades."
- Check Point offers wide and consistent support across platforms, including desktops, notebooks, smartphones and tablets. Check Point has been early to market for several years, with optimized support for smartphones and tablets.
- Native support for Microsoft Exchange is present in the VPN gateway so that users do not need a direct connection to an internal Exchange server to synchronize. However, most Gartner clients prefer to select a mobile device management (MDM) vendor to help with this task.

Cautions

- Reported and estimated SSL LOB performance and visibility have been below average. Gartner clients that inquired about SSL VPNs were likely to ask for a replacement or a different vendor for SSL, even if they use Check Point firewalls. Clients reported confusion over pricing and requirements for VPN client software, as well as variable support quality from resellers.
- Despite Check Point's innovations during the past several years, its efforts have not made the company stronger in terms of competitive recognition by vendors or buyers. Based on client feedback and peer analyst review, Gartner believes it merits a Visionary ranking.
- A next-generation "VPN on a stick" named Abra was delivered, but SanDisk decided to cancel the original partnered Cruzer hardware product. Check Point has gone through a brand change to the name "Go" and has rereleased Go to include portable applications. It is also planning to support Go on other hardware devices beyond SanDisk. Check Point has had some successful Go deployments, but in general, Gartner believes that demand for and visionary value of all products in this class have diminished since last year.

Cisco

Cisco released its first SSL VPN in 2004. Today, Cisco's SSL VPN capabilities are an embedded option on all Adaptive Security Appliances (ASA series) and many Cisco IOS platforms. Cisco's universal-access vision for VPNs is embodied in AnyConnect, a ubiquitous VPN client that enjoys a tacit endorsement from Apple for use on iPhones and iPads. It is also available on other mobile device platforms, including Android, Symbian and Windows Mobile 6.x, in addition to PCs, Macs and Linux. Cisco's product focus and vision are expressed in the Secure Mobility solution, and it has been well-communicated to buyers and has received a strongly positive response from users. FIPS 140-2 certifications of several levels are offered on different hardware and software platforms. Most ASA platforms are certified to Level 2 and garner CC EAL4. AnyConnect client is certified to Level 1 and CC EAL4.

Strengths

- Cisco currently generates a high rate of Gartner client inquiries, and earns a high level of client awareness. Among legacy network infrastructure players, Cisco is highly successful at generating revenue for both IPsec and SSL VPNs because of the low cost and ease of activation on ASA platforms, as well as the positive end-user experience, particularly on mobile devices. Cisco's SSL VPN entry cost and discount rates are the lowest reported in the history of this Magic Quadrant report. Other surveyed vendors consider Cisco a major competitive threat, which shares second place with Citrix Systems after Juniper Networks.
- AnyConnect offers basic network persistence for unstable connections. It supports an automatic connect mode to compete with Microsoft DirectAccess and a connect-on-demand mode to support power savings and mobile access needs.
- Cisco's 2010 and preliminary 2011 VPN LOB revenue results are the second highest reported. Overall seat penetrations are the highest reported for several years, and would be ranked at the top even if the count was conservatively discounted. Cisco sells in all geographies for all use cases, and is adept at selling SSL VPN combined with or as a total replacement for IPsec.

Cautions

- Low pricing combined with high volume may set a limit on the revenue that Cisco can generate from the SSL VPN portion of the ASA platform and may lead to buyer saturation. In contrast, some other influential vendors derive a high rate of revenue from SSL VPN. Buyers should make their deals while the deals are good, so to speak, because there are valid competitive reasons for a future price hike.
- Despite a strong ranking in the "Magic Quadrant for Secure Web Gateway," Cisco ScanSafe Secure Mobility doesn't generate visibility among Gartner clients in a manner commensurate with ScanSafe's role in protecting remote-access users. Buyers should consider Cisco ScanSafe Secure Mobility when setting up SSL VPNs with the Cisco AnyConnect client.
- Cisco buyers have long upgrade wish lists in line with leadership expectations. Buyers should ask for road map commitments for leading-edge concerns — including universal Android SSL support (that is, for all Android variants on the market); enhanced management in bring your own device (BYOD) scenarios; and integration with Cisco Identity Services Engine (ISE), which supersedes Cisco Network Admission Control (NAC).

Citrix Systems

Citrix built its Citrix Access Gateway and Citrix NetScaler products to provide secure remote-access enterprise and Web applications, including virtualized applications and desktops. Buyers primarily use Citrix SSL capabilities to extend secure access to XenApp or XenDesktop. Citrix Access Gateway Enterprise Edition has been natively certified to CC EAL2 and up. Starting in 2011, SSL is being repositioned as an embedded feature in other product lines, including XenDesktop, XenApp, NetScaler and CloudGateway. Future development efforts will mix internal and external application access to Web, Windows, software as a service (SaaS), and mobile apps and data at Citrix CloudGateway. Although Citrix chose not to participate in this year's survey, a combination of empirical evidence from industry sources, client feedback, and Gartner's prevailing knowledge of Citrix use cases and capabilities merited its ranking in this Magic Quadrant report.

Strengths

- During the study period, Citrix SSL VPN gateways generated significant enterprise market presence and user interest. These gateways are frequently bundled with sales for XenApp and XenDesktop through strong global reseller channels. Citrix shares second place with Cisco in being named a competitive threat among the surveyed vendors.
- Citrix Receiver is a well-known remote application display platform and supports a wide range of end platforms, including smartphones and tablets. It is frequently used as an enabler for remote access to XenApp. Features such as SmoothRoaming enhance the stability of Receiver when operating through a VPN.
- Citrix provides an unusually broad choice for management interfaces, including a proprietary console delivered via Flash, Microsoft Management Console (MMC) snap-in, programmable SOAP interface and SNMP. Citrix also provides integration with security information and event management (SIEM) products that have syslog and SNMP hooks.

Cautions

- IT managers are unlikely to recognize Citrix as a player in the VPN market. IT managers frequently contend with two VPNs: one intentionally purchased for network infrastructure; and the other — a Citrix product — independently introduced by the application team. Indirect selling and duplication do not generate competition, according to a clear pursuit of the market definition used in this report; therefore, execution has been reduced.
- Citrix has repositioned its new access solutions to be features of CloudGateway, in ways that increasingly diverge from the market definition used in this report. CloudGateway is an important strategic vision for Citrix, but the SSL VPN offering equates to a Challenger ranking in the prevailing SSL VPN Magic Quadrant definition.
- Competing SSL VPN vendors can offer access support for XenApp and XenDesktop that is similar to the Citrix gateway experience, including selective application publishing at a low incremental cost on top of existing SSL VPNs.

Cryptzone

In 2010, Cryptzone acquired AppGate, a relatively small company with market share and other criteria sufficient for inclusion in this Magic Quadrant. AppGate began building secure access solutions for the Swedish defense industry in the late 1990s. The VPN provides functions, look and feel that are highly similar to a typical SSL VPN, but it uses SSH as the underlying transport layer. This is acceptable because some Gartner clients are interested in SSH for VPNs. Cryptzone provides additional funds and resources and is building a presence in U.S. markets. Buyers are most interested in extranet/contractor access, nonbrowser tunnel clients and smartphone VPNs. AppGate features an embedded FIPS 140-2 Level 1 validated cryptographic module based on OpenSSL 1.1.2. Products are certified to CC EAL2 and up.

Strengths

- AppGate becomes the secure access component within Cryptzone's larger portfolio of security solutions, which include risk management, policy compliance, content security and endpoint security.
- For a small company, Cryptzone has offered complex and varied references, indicating an ability to compete on mission-critical real-time implementations. Mobile clients are available for all major phone and tablet platforms, including Apple and Google.
- The company has been able to reduce its reliance on European trade and is showing notable revenue growth in North America, the Middle East and Africa.

Cautions

- Acceleration is not available at this time from AppGate, although compression is included.
- AppGate does not support a connect-on-demand VPN, and should add this capability to support roaming mobile-device-access scenarios.
- Its revenue for 2010 to 2011 is at the bottom of the range of ranked vendors, although well within the inclusion level. However, in a mature market, the ranking prospect remains as a Niche Player.

F5 Networks

F5 has offered SSL VPNs since 2003. F5's main distinguishing characteristics are high performance, reliable gateways and carrier-class acceleration. F5 delivers steadily on road map milestones, including its Access Policy Manager (APM), Big-IP Edge Gateway and support for mobile devices. Combined with good feedback, breadth of deployments and seat penetration exceeding 1 million for the past year, F5 regains its Leader ranking. Buyer preferences include hosted virtual desktop support, business continuity and smartphone support. Big-IP earns a certification of CC EAL2 and up; FIPS 140-2 Level 1 certification on all models can be provided by optional hardware.

Strengths

- Revenue for F5's SSL VPN LOB grew a solid 28% in 2010, following a strong run of 35% growth during the economic slowdown of 2008 and 2009. Overall, the company grew more than 40% after a flat performance in the study period of the previous Magic Quadrant report.
- F5's ability to sell a general-purpose remote-access solution, a strong understanding of Web application deployments within the enterprise, and the fact that it is a leading player in the provision of application delivery services account for a healthy ranking for vision. F5 is a strong player in related markets for load balancing, Web acceleration, WAN optimization, dynamic DNS load balancing, application-level failover and Web application firewall. Entry-level pricing is attractive. Top-end performance reaches 60,000 user sessions in a single appliance, supporting throughput speeds of 10 Gbps and up.
- F5's Visual Policy Editor and iRules scripting language continue to set the bar for ease of use and user-driven customization. Visual support has been expanded to iApps for application delivery.
- Native agent support was added in 2011 for Apple and Google phones and tablets.

Cautions

- F5 receives a third-place mention as a competitive threat by its peers, which is indicative of selling into different buying centers, on the positive side, but of missing opportunities to compete, on the negative side. The competitive threat question is indicative of the ability of a vendor to be disruptive in a market.
- F5 faces an uphill contest with vendors that offer both SSL and IPsec, and should reconsider whether to build or acquire client-based IPsec support, particularly to meet a wider set of needs on mobile devices.

Juniper Networks

Juniper Networks has held a Leader position continuously since entering the Magic Quadrant report in 2004. Juniper competes on the basis of universal access, broad client platform support and comprehensive infrastructure. The Secure Access SSL VPN hardware product line can scale to hundreds of thousands of users and sells well to carriers and application service brokers, in addition to enterprises. Buyers prefer Juniper SSL as a total replacement for IPsec and for extranet/contractor access. All products are natively certified to CC EAL3 and up. A FIPS 140-2 Level 3 cryptographic module is available on selected models.

Strengths

- Juniper delivers sound multiyear performance, with strong sales and revenue in SSL and IPsec VPNs. In general, Juniper can sell products at a high rate, with higher incremental revenue than any other company in the market, creating an unchallenged disruptive sales advantage. Juniper's current historical revenues are the best in the SSL VPN market, and a high client satisfaction rate keeps buyers on the platform.

- Juniper is the No. 1 competitive threat cited by peer vendors in the SSL VPN market. This assessment has persisted for many years. Juniper sells in all geographies for all use cases. The company appears on most shortlists discussed in Gartner client inquiries for midsize to large businesses and is entrenched in the Fortune 500, with a track record for large deployments.
- Juniper's Junos Pulse client, introduced in October 2010, has been highly visible in client planning decisions for mobile phones and tablets, with support offered for Apple and Google devices. On PCs, Pulse supports an automatic connection mode to compete with Microsoft DirectAccess.

Cautions

- Juniper's entry prices continue to be high in the market, but are negotiable. Various competitors are more effective at selling to the small-business end of the market because of lower entry prices.
- Clients reaching end of life on their Juniper VPNs have reported that upgrades and replacements are typically not discounted.
- The Junos Pulse Mobile Security Suite and the Junos Pulse Secure Access Service for SSL VPN share a common umbrella brand in Junos Pulse, though the Mobile Security Suite and mobile VPN can work entirely independently. Sometimes, customers have been confused over this point. Because VPN and MDM are still separate buying centers, the confusion can delay product selection.

Microsoft

Microsoft has offered SSL VPN support since 2006, based on technology acquired from Whale Communications, starting with the Intelligent Access Gateway (IAG), and followed by the Unified Access Gateway (UAG). Buyers frequently pick UAG to provide secure access, in combination with SharePoint and Forefront. UAG is certified to CC EAL2 and up, and uses the Windows cryptographic functions, which are compliant with FIPS 140-2.

Strengths

- Microsoft's UAG has proved to be a dependable product, and earns positive client feedback. Microsoft has been successful at selling UAG into small, midsize and large businesses.
- Deep interoperability with the Windows OS and many Microsoft product families is an advantage for IT organizations that are intent on comprehensive Windows solutions. Specifically, Microsoft provides its own UAG application optimizers for Exchange (Outlook Web App, ActiveSync and Outlook Anywhere), SharePoint, Dynamics CRM, Lync, Remote Desktop Services and Forefront Identity Manager. Third-party optimizers are offered through partners for SAP, IBM Lotus Notes and others.
- Multiple gateways may be clustered for management purposes in large-scale installations.

Cautions

- Microsoft is promoting DirectAccess as an alternative to a VPN. Conceptual differences between conventional VPNs and Microsoft DirectAccess are confusing and sometimes helpful to the competition. Other VPN vendors have prepared explanations for creating the equivalent experience to DirectAccess by using automatic connection methods.
- During the study period, Microsoft did not offer a full UAG-managed, value-added VPN with endpoint detection and management for Windows Phone 7 or other smartphone platforms. Outside of UAG, Microsoft can publish Exchange ActiveSync and SharePoint to Windows Mobile, Windows Phone 7, Android, Apple and Symbian devices.
- Microsoft does not currently provide direct support to an independent, trusted time and date source to validate the audit trail from its management system.
- Microsoft does not provide comparative estimates of revenue or penetration. Based on client feedback and peer analyst review, Gartner believes it merits a Visionary ranking.

Sangfor Technologies

Sangfor Technologies is a competitive specialist for VPN products and services, originating in China. In addition to SSL VPNs, Sangfor provides IPsec VPNs, WAN optimization, Internet access management, IT governance audits and Internet law assistance. Sangfor has extended its operations with local presence in the U.K., Singapore, Thailand, Malaysia and Hong Kong. Buyers respond most strongly to IPsec replacement, extranet/contractor access solutions and SSL client security features. All products are security-certified by the Chinese government.

Strengths

- Sangfor is a native Chinese company, and claims to have a presence in 70% of the top 500 businesses in China. Its revenue is currently derived 100% in Asia/Pacific, but the company has opened operations in the U.K., Singapore, Thailand, Malaysia, Indonesia and Hong Kong. In China, Sangfor has rolled out 34 direct branches and approximately 436 partnership agencies for sales and support.
- Revenues in the SSL VPN LOB, as well as seat sales, are on par with some of the established smaller, long-term strong Niche Player and Visionary companies in this Magic Quadrant. Seat sales doubled in 2010 over 2009. Revenue in the SSL VPN LOB was essentially flat, but overall revenues grew by 32%, compared with the study period in the previous Magic Quadrant report.
- Pricing is competitive with many of the incumbent vendors tracked in this market, particularly where expertise in China is a factor. Sangfor can offer advantages for companies that wish to operate VPNs going in and out of China. Companies that wish to do business in China will need to comply with China's regulations for privacy and security.

Cautions

- As a native Chinese company, Sangfor has considerable experience and authorization to sell VPN products under regulation by the Chinese Ministry of Public Security and Office of the State Commercial Cryptography Administration (OSCCA) for certification of its commercial password product. Buyers who are expanding their presence in China will benefit from Sangfor's knowledge. However, multinational companies that choose products operating under Chinese regulations should closely examine the crossover point between Chinese regulations and other countries.
- Sangfor offers a broad product portfolio, along with the strength of its specifications and a strong business built within China, which merits an execution rating that is on par with similar performers. However, its narrow geographical operation limits competitive options, regardless of other vision factors, earning it an overall Niche Player status in this report.
- Sangfor does not yet have provisions for rapid surge access to the VPN, requiring fast scaling, to support business emergency situations.

SonicWALL

SonicWALL sold SSL and IPsec VPNs into small and midsize businesses before acquiring Aventail in 2007. The company sells VPN products under both brand names, with Aventail products serving the high end. SonicWALL was acquired by Thoma Bravo in 2010, and operates again as a private company for the first time in 10 years. The transaction provides SonicWALL with financial protection and a stable base for future growth. Buyers are strongly interested in deploying VPNs for vertical applications and extranet/contractor access, leveraging SSL convenience. FIPS 140-2-level-certified encryption is natively provided on selected appliance platforms.

Strengths

- SonicWALL sells primarily in North America, but has a global presence and global support structure.
- SonicWALL's 2010 seat penetrations and forecast for 2011 are showing good growth, up 50% relative to the study period in the previous Magic Quadrant report. This growth helps the company catch up from a loss of growth caused by the economic slowdown of 2008 and 2009, but it is not enough to earn Leader execution.
- SonicWALL has preferred status to sell its products to other companies in the Thoma Bravo portfolio, some of which are already large customers. Additionally, SonicWALL continues to sell Aventail products to global carriers, which use its products to build managed remote-access services.

Cautions

- SonicWALL's 2010 LOB revenue is increasing but remained low, compared with other long-term vendors with foundational products in the VPN market. The company's SuperMassive platform has not generated significant Gartner inquiries regarding new investments, nor has it reduced inquiries about enterprise product replacement.

- SonicWALL was able during the study period to integrate basic security policy management with ActiveSync on popular smartphones, but is still working to broaden full support for mobile platforms. Mobile support has improved in the latest releases, and a Mobile Connect client was released for Apple mobile devices in December, after the close of the survey.
- SonicWALL is missing opportunities by not leveraging intelligence in the information it collects from more than 1 million managed customer gateways to analyze and publicize Internet security and performance statistics in business-relevant remote-access contexts.

Technology Nexus

Technology Nexus is the merger of Nexus and PortWise. PortWise has sold mobile VPNs since 2000 and gained an early foothold in mobile banking. The merger has established a broader product portfolio, as well as added to financial stability. Buyers respond most strongly to use cases such as extranet/contractor access, disaster management/business continuity and vertical applications. The FIPS 140-2-certified cryptographic module is supported by means of third-party cards offered as an add-on to a standard license.

Strengths

- Technology Nexus' 2010 SSL VPN LOB revenue grew by 19% over 2009 in line with the median improvement reported by vendors in this survey, and the company overall grew 35% since the previous Magic Quadrant report. Operations have also diversified significantly since then, with roughly equal revenues coming from Europe, Asia/Pacific and the Americas.
- Technology Nexus has extensive experience in delivering secure services and applications to handheld wireless devices, including a long track record with sensitive applications (such as retail banking and credit card terminals) and industrial applications (such as vehicle management).
- Technology Nexus is among the few vendors that offer in-house, integrated, one-time password tokens in the user interface.

Cautions

- The company is rarely mentioned on shortlists for SSL VPN or mobile VPN.
- Seat sales are sufficient for inclusion and, in fact, grew 60% since the previous Magic Quadrant report, but are at the bottom end among ranked vendors.
- Technology Nexus does not currently provide a trusted time and date source to validate the audit trail from its management system.

Ultra Electronics

In September 2011, Ultra Electronics announced it had acquired AEP Networks. Both Ultra and AEP specialize in niche markets — AEP particularly in government sales. AEP sells primarily in European markets, with some presence in North America. Buyers are strongly interested in VPN replacements and business continuity solutions. Several of the hardware products are natively certified to a relatively high cryptographic level. Notably, the Series K Hardware Security Module has achieved FIPS 140-2 Level 4.

Strengths

- AEP's 2010 VPN revenue is growing, along with overall company revenue, after several flat years. AEP had a steady market presence, long track record, and reliable products that have sold on a par with specialized niche vendors. Ultra Electronics is expected to contribute to viability.
- AEP has emphasized policy-based security and high certification levels, and robust key management.

Cautions

- New owner Ultra Electronics specializes in niche military applications for aircraft and vehicle systems, information and power systems, and tactical and sonar systems. These use cases diverge from the enterprise market, which typifies vendors tracked in this report.
- AEP's seat penetrations for 2007 through 3Q11 remain at the low end of those reported in the surveys. In combination with other evaluation factors, such as high-security specialization, they contribute to reduce its market visibility, influence and vision.
- AEP offers load balancing but not other optimization performance enhancements, such as SSL acceleration, WAN optimization, bandwidth throttling, compression and caching.

Recommended Reading

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

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

"Toolkit: Secure Sockets Layer Virtual Private Network RFI and RFP Templates"

"Forecast: Specialized SSL VPN Equipment, Worldwide, 2005-2015, 4Q11 Update"

"Forecast: Enterprise Routers and IPsec VPN/Firewall Equipment, Worldwide, 2005-2015, 4Q11 Update"

"Cautionary Planning for Mobile VPNs on Consumer Smartphones and Tablets"

"Q&A: Windows 7 DirectAccess Challenges Remote-Access VPNs"

"Magic Quadrant for Secure Web Gateway"

"Q&A: Implementation Advice for SSL VPNs"

"'Panning for Gold' Outside the Leaders Quadrant of Gartner's Magic Quadrant"

Vendors Added or Dropped

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

Evaluation Criteria Definitions

Ability to Execute

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

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood of the individual business unit to continue investing in the product, to continue offering the product and to advance the state of the art within the organization's portfolio of products.

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

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

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order 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, 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, etc.

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

Completeness of Vision

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

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

Sales Strategy: The strategy for selling product 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 set 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 verticals.

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

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

Regional Headquarters

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

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

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

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

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

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