



# Magic Quadrant for SSL VPNs

11 December 2008

John Girard

Gartner RAS Core Research Note G00163232

Secure Sockets Layer virtual private networks continue to lead the remote-access VPN segment for competitive growth and innovation.

## What You Need to Know

Remote access creates continuous market demand for new virtual private network (VPN) products and services. Every company is working through upgrade and replacement cycles that bring opportunities to replace legacy remote-access VPNs as well as in-between cycle projects such as business continuity and telework. IPsec VPNs are still popular for remote access, but the most interesting and visible market innovations continue to center on using Secure Sockets Layer (SSL) VPNs as replacements or augmentations for legacy VPNs. IPsec VPN products have never caught up with SSL in terms of ease of implementation, policy and network access controls, and the ability to deliver security protections on demand. SSL VPNs are easy to set up in their default role as application portals, and offer decent performance for tunneled Layer 3 traffic. Market definitions follow the competition and the money. In the case of remote-access VPNs, SSL products and services set the pace, and Gartner will continue to track growth of the market primarily in terms of SSL.

Gartner ranks vendors in the Magic Quadrant (see Figure 1) based on performance for calendar year 2007 through the end of September 2008 and on client reviews received up to October 2008. The Magic Quadrant considers which vendors likely will dominate remote-access VPN sales and influence technology directions through 2013, as well as which vendors are most visible among clients, generate the greatest number of requests for information and contract reviews, and account for the most new and ongoing installations in Gartner's client base.

After reading this Magic Quadrant:

- Consider the merits of all the vendors in the report. All vendors that Gartner tracks in the SSL VPN market have good products that will meet the needs of most buyers.
- Consider your incumbent vendors. There can be benefits for not adding another contract as well as avoiding a new console and new training. If an additional vendor is the best choice, be prepared to justify your claims.
- Look for differentiating features based on your business requirements, such as network access control, high-end scalability, acceleration and load balancing, management interfaces, security certifications, endpoint security, and partnerships.
- Consider vendor ratings, strengths and challenges in adjacent markets such as WAN optimization, application delivery, Web conferencing, and enterprise single sign-on.
- Ask for and contact customer references.
- Decide what you are willing to pay. Negotiate your initial purchase price based on a future commitment, and include no-penalty escape clauses in case the product and the vendor fail to deliver service levels.

[Return to Top](#)

## Magic Quadrant

Figure 1. Magic Quadrant for SSL VPNs

### 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 and so on, 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.

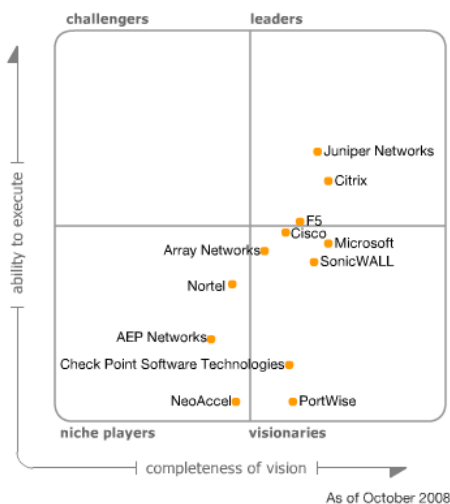
**Market Responsiveness and Track Record:** Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

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



Source: Gartner (October 2008)

[Return to Top](#)

### Market Overview

SSL VPNs are persistent encrypted connections between user systems and VPN gateways to Layer 7 access to applications and Layer 3 access to networks. SSL VPNs typically feature a menu-driven front end to provide a default greeting to a remote user. The front end is driven by rules that determine the resources that will be offered to the user. Access choices made by the user can be logged at a granular level, because the user is not automatically bridged to the LAN — as would be the case with IPsec.

SSL VPNs were conceived to make it easier for users to install and understand their options, and more reliable under the variable quality conditions of remote access. The original concept of an SSL VPN was to use the browser as the entry point. Browsers facilitate extreme VPN portability and flexibility:

- They are found on every platform.
- All browsers contain embedded encryption (SSL) and certificate authentication.
- Several mechanisms are included to download executable code on demand that can be used to enhance the VPN.
- Browsers drive demand for interoperability and compatibility.
- They are optimized to facilitate application delivery over unreliable network connections.

SSL VPNs have, of course, evolved beyond basic browser access. The basic value proposition for SSL VPNs has been made stronger because of several critical capabilities:

- The VPN can be established without a formally installed client beyond the browser.
- Sessions can survive multiple interruptions and can reconnect and roam across networks without preserving an Internet Protocol (IP) address.
- The strength of SSL encryption has been enhanced to conform to current standards.
- Security applets can be downloaded to end-user systems during session establishment to perform policy checks, network access controls, tunnel controls and data protection "on-demand."
- On-demand security applets can enforce policies and set access limits, even on completely unmanaged systems, without formally installing additional software.
- Nonbrowser SSL VPN clients, available today, give users a similar experience to legacy IPsec VPNs while adding the flexibility of SSL.

Gartner is no longer anticipating that SSL will cause a downturn in the use of IPsec for remote access, because:

- IPsec has inherent advantages of efficiency. IPsec tunnels require less gateway overhead and scale better than SSL.
- It is deeply embedded in networking products such as routers and firewalls, and, therefore, has a lower incremental session cost in gateways.
- IPsec is easier on battery life in handheld devices, if persistent network tunnels are required.
- Microsoft, Nokia and Apple include mobile IPsec clients. Several major and specialty independent software vendors (ISVs) offer mobile VPNs based on IPsec and proprietary protocols. The low barrier to entry to start with these products delays consideration for SSL VPNs.

However, we do believe that SSL VPN agents define the preferred future of portable VPN "agents" for establishing remote-access connections for several important reasons:

- Open-source IPsec clients have no appeal to replace browser-based security managers. Major vendors with proprietary IPsec clients have little motivation to facilitate interoperability. The only way to be as good as an SSL client would be to duplicate the architecture.
- IPsec clients and gateways from different vendors do not mix well because of differences in default configurations. With IPsec, the client configuration for one vendor may be difficult or impossible to modify or fully support the configuration of another vendor's gateway. With SSL, each gateway vendor can negotiate its own terms for client configuration at the browser through basic browser settings and downloadable ActiveX and Java agents.
- SSL VPNs from vendors that support IPsec can launch SSL-managed IPsec tunnels as desired for high-throughput Layer 3 demands. IPsec sessions managed by SSL clients will not suffer the problems of legacy IPsec VPNs, such as instability on poor quality networks and reliance on IP addresses for validation.

**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 Web site, 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.

Gartner forecasts that revenue from SSL VPN equipment will grow at a compound annual rate of almost 14% between 2007 and 2012, with growth peaking at 22% during 2009. Market size was \$438 million in 2007, with a forecast of \$506 million for 2008 (see "Forecast: Specialized SSL VPN Equipment, Worldwide, 2005-2012"). Data collected in the 2008 Magic Quadrant survey is consistent with this estimate, and somewhat enhanced when considering related VPN markets and services. Seat sales or penetrations (usable VPN session seats, counted in sales of license numbers or estimated by the normal session capacity of the gateways sold) in the SSL VPN market reported by the 12 surveyed vendors, as well as historical data, are estimated to claim more than 5.7 million seats in 2007, and the first three quarters of 2008 are already estimated at 5.3 million. Total seats counted for the years 2005 through 2007 now exceed 10.8 million.

Many companies are still working through their investment life cycle of legacy VPNs, and upgrade/replacement opportunities will continue through the coming years as companies reach end of life on their legacy VPNs and seek easy ways to expand new VPN connections. Dedicated VPN appliances have a useful life of more than five years, as long as Windows Vista, Windows 7, Apple and Linux can be accommodated, and the vendor does not declare end of life for support. All vendors can pick up new business as the cycles retire, but vendor selling skills will be tested to qualify buyers at the right time and place.

Application-driven access for specific tasks is a growth opportunity that expands beyond conventional VPNs to include single-application access, such as e-mail and secure Web application portals for business-to-business and business-to-consumer applications. SSL VPNs are highly adaptable for application delivery purposes. Sales for these purposes require entry into different buying centers than are typical for VPNs. Citrix is clearly the company most prepared to sell in this manner, and the company's high performance in seat sales and revenue proves this point. Similarities in future vision and road map responses from Array Networks, F5, Juniper Networks and Microsoft indicate a willingness to follow Citrix into the application-driven model.

[↩ Return to Top](#)

## 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 PDA or smartphone. This Magic Quadrant evaluates SSL VPN products that are sold for purchase and use within enterprises.

All companies that sell IPsec remote-access VPNs were asked about their experiences in selling the two different types of VPNs. With one exception, all vendors believed that SSL VPNs provided the most significant current and future growth opportunities. The contribution of IPsec remote-access VPN revenue proved impractical to quantify as an execution differentiator because, as mentioned, IPsec is embedded in router and firewall appliances, and the purchasing decision can no longer be separated for competitive analysis.

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, particularly VMware, which makes it easy to develop drop-in, scalable, plug-and-play solutions for gateway production systems as well as easily accessed, presales 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 VPNs, and a few companies omit the menu interface altogether.

SSL VPNs support the strong authentication and logging desired for VPN protection as well as application access audits, and support the roaming required for mobile users.

Since 2007, sales are seen to be increasing all over the world; even the smaller vendors are building presence in multiple geographies.

Services built from the products and offered by third parties are considered additive to the product vendor ranking, but did not drive the evaluation. Managed network services of all types are separate markets.

[↩ Return to Top](#)

## Inclusion and Exclusion Criteria

### Inclusion Criteria

SSL VPN companies that meet the market definition and description were considered for this research under these conditions:

- Gartner analysts have a generally favorable opinion about the company's ability to compete in the market.
- Gartner clients generate inquiries about the company.
- The company causes clients to change or delay their procurement plans for competing products.
- Competitors regard the company as a serious threat.
- The company regularly appears on shortlists for final selection.
- The company demonstrates a competitive presence and sales to Gartner analysts.
- Gartner analysts consider that aspects of the company's product execution and vision are important enough to merit inclusion.

For 2008, the minimum thresholds for seat sales and revenue were not applied.

### Exclusion Criteria

SSL VPN companies not included in the 2008 Magic Quadrant might have been excluded for one or more of these conditions:

- The company did not have a product on the market for a sufficient time during the study period to establish a visible, competitive position.
- The company was invited to participate, but did not reply to an annual request for information and did

not otherwise meet the inclusion criteria.

- The company had a minimal or negligible apparent market share and market inquiry interest among Gartner clients, or had no products shipping.
- The company sells the product as an application firewall and is not competing directly within the larger SSL VPN product/function view.
- The company sells SSL accelerators and load balancers as stand-alone products for other purposes besides SSL VPNs.
- The company sells Web-enabled personal remote-control products that are not true multiuser access gateways.

#### Other Companies

Several companies are on a list for re-evaluation for possible inclusion in the 2009 Magic Quadrant. Factors that affect inclusion (as listed in this Magic Quadrant) include client inquiry, competitive reaction from peers, market visibility and market share. The list includes Aladdin Knowledge Systems (acquired Secure Computing's VPN and authentication business), AppGate Network Security, Fortinet, NCP engineering, Stonesoft and WatchGuard Technologies.

[Return to Top](#)

#### Added

None.

[Return to Top](#)

#### Dropped

None.

[Return to Top](#)

### 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 and also on comments from each vendor about its peer group. For example, in 2008, Juniper Networks, Cisco and Citrix are considered the most serious competitive threats among peers. The level of concern for other vendors is negligible in comparison.

**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 versus 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 50 concurrent users 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.

Low pricing does not guarantee high execution or client interest, and the market, as a whole, did not move to commodity status in 2008, although Cisco continued into a two-year unprecedented spike in low-cost seat sales. Buyers want good results more than they want bargains, and they respond more strongly to sales techniques led by case studies and return-on-investment projections.

**Market Responsiveness and Track Record and Marketing Execution:** Rates competitive visibility as the key factor, including which vendors are most commonly considered top competitive threats during the RFP process and which are considered top threats by each other. 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 of competition with other vendors. Marketing execution in this report is considered an aspect of market responsiveness and track record rather than a separate criterion.

**Customer Experience:** Is subjectively rated from clients' 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 (October 2008)

[Return to Top](#)

### Completeness of Vision

**Market Understanding and Marketing Strategy:** Assessed through direct observation of the degree to which a vendor's products, road maps and mission anticipate leading-edge thinking about buyers' 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 operating-system support for the SSL client, the VPN gateway operating system 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 verticals.

**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 (October 2008)

[Return to Top](#)

## Leaders

Leaders demonstrate balanced progress and effort 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 mobile access 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.

[↩ Return to Top](#)

## Challengers

Challengers have solid products that address the typical needs of the market with strong sales, visibility and clout that add up to higher execution than niche players. Challengers are good at winning contracts, but they do so by competing on a basic or limited selection of functions rather than on advanced features. Challengers are efficient and expedient choices for defined access problems. Many clients consider challengers to be the conservative, safe alternative to niche players.

[↩ Return to Top](#)

## 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. Clients pick visionaries for best-of-breed features, and, in the case of small vendors, may obtain more personal attention.

[↩ Return to Top](#)

## 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 when stability and focus on a few important functions and features are more important than a wide and long road map.

[↩ Return to Top](#)

## Vendor Strengths and Cautions

### AEP Networks

#### Strengths

- AEP Networks has hardware products that are certified to a relatively high level: Federal Information Processing Standard (FIPS) 140 Security Level 4.
- The company's products appeal to departmental and small/midsize buyers that want a small number of seat licenses and to government buyers seeking high levels of certification.
- Its gateway server can run on VMware.
- AEP has a steady market presence, long track record and reliable products that emphasize policy and access controls.

[↩ Return to Top](#)

#### Cautions

- AEP's revenue for 2007 and 2008 is relatively low, but healthy, in keeping with the execution of a stable niche player and long-established company.
- AEP follows all the major directions of the market, but does not set directions nor force others to react. This mode of operation is in keeping with the vision of a niche player.
- Its seat penetrations for 2007 and 2008 are among the lowest reported. This may provide opportunities to upsell into existing accounts, but must be considered to reduce market visibility and influence.

[↩ Return to Top](#)

### Array Networks

#### Strengths

- Array Networks has competitive price/performance and scalability for large and demanding access needs, while also offering an affordable, low-end entry point. Array's Universal Access Controller and secure access and application delivery solutions road maps are dedicated to growing a seamless product line with "green" IT values.
- Its core capabilities in acceleration and load balancing contribute to viability.
- Array added innovative, wireless overlay security management and wake-on-LAN remote control to its product lineup in 2008 — both being popular areas of concern for access control.

[↩ Return to Top](#)

### Cautions

- Array is mentioned rarely by Gartner clients and is not considered a competitive threat by peers. Array must increase the effectiveness of its marketing and communications, and must be seen frequently in head-on competition in Gartner client RFPs with companies ranked as leaders.
- Array's revenue and seat shares grew in 2007 and 2008, but are below the average.
- Its revenue for 2007 and 2008 is more in line with visionary players and is spread through the addition of products for wireless LANs and remote control. However, its new product directions are additive to its Universal Access Vision.

[↩ Return to Top](#)

## Check Point Software Technologies

### Strengths

- Check Point has a complete and well-designed product, with a comprehensive set of on-demand security features and a unified IPsec/SSL client.
- It has added embedded support for Short Message Service (SMS) one-time passwords.
- Its gateway is available as software, a hardware appliance and as a VMware ESX Server virtual appliance.
- Its broad features for handheld platforms include local Bluetooth and firewall controls.
- Check Point's operating system is certified for FIPS 140-2 and Common Criteria (CC) Evaluation Assurance Level (EAL) 4. Certification updates are in process for Check Point VPN-1 Power/UTM NGX R65 with SNX.

[↩ Return to Top](#)

### Cautions

- Business revenue for SSL products is below average for 2007 and the first half of 2008. Given the size, visibility and reach of the company, as well as work on a major new Connectra release, execution was expected to show more strongly. At this point, performance on revenue and seat penetrations is more on a par with smaller companies.
- Connectra is not certified for FIPS 140 or CC and there is no optional FIPS-certified crypto module from a third party. However, FIPS 140 certification is planned for next year.
- Gartner clients that inquired about SSL VPNs were likely to consider a separate vendor for SSL, even if they use firewalls or IPsec from Check Point.

[↩ Return to Top](#)

## Cisco

### Strengths

- Cisco's estimated seat penetration for SSL VPN in 2008, on sheer numbers alone, is very high, just behind Citrix. Also, Cisco's entry cost per seat is the lowest reported.
- Nine out of 12 vendors consider Cisco a major competitive threat, earning Cisco second place after Juniper as a named competitive threat.
- Its Adaptive Security Appliance (ASA) platforms offer sufficient resources to support a practical and attractive combined capacity for IPsec and SSL with further optimizations for voice and video.
- All Cisco's ASA 7.2.2 platforms include FIPS 140-2 certification. ASA 8.1 is in prevalidation phase. CC EAL 4 is in process.
- Cisco's future road map is loaded with compelling features including expanded support for mobile platforms, roaming, optimization and new scalable/virtual architectures.

[↩ Return to Top](#)

### Cautions

- Cisco's increasing sales performance cannot yet be directly counted toward leader-class execution until other execution factors align on competitive merits. For example, client feedback and independent investigations can't verify that these seats are all assigned for use, or are causing other vendors, particularly high-end leaders Juniper Networks and Citrix, to lose competitive deals or market share.
- Cisco was a relatively late entrant among major vendors and played "catch up" on features into 2007.
- Publicly documented case studies and use-based sales and marketing messages have been scarce. Cisco needs to put more effort into documenting its success stories.
- Gartner clients have reported purchasing other vendors' VPNs for specific business projects even when Cisco's product is already installed with SSL licenses, or readily upgradable. This is a symptom of the disconnect between buying centers for application delivery purchases and pure network access, and may indicate that in some cases SSL is purchased incidentally, rather than intentionally. Cisco needs to escape legacy perceptions that limit buyer awareness of its breadth of product features.

[↩ Return to Top](#)

## Citrix

### Strengths

- Citrix has the greatest experience of all market vendors in remote, thin-client application delivery. In the 1990s, the company developed the original, protected browserlike client (SecureICA) well ahead of the SSL VPN market, and has the longest commercial experience with screen-oriented security, such as the

ability to block cut and paste.

- Citrix Access Gateway is built from the best of technologies acquired from Caymas in 2007 (traffic inspection and acceleration), Net6 (SSL optimization and VoIP), and Netscaler (carrier-class hardware).
- Xen virtualization technologies are being applied in compelling ways at the gateway server side as well as the client side. With XenApp, Citrix can offer hosted and streamed Windows applications across a wide range of end-user devices. When XenApp streams applications, it runs them in a local isolation environment with security policies set and managed by the Citrix Access Gateway.
- Leading sales and market share do not depend on selling to legacy VPN buyers. Citrix is leading sales in application delivery areas generally closed to networking equipment vendors. In our opinion, the efforts by vendors other than Microsoft to follow Citrix on grounds of application delivery have been uncompetitive.
- Citrix revenue performance was second highest in the survey. Seat penetrations are also very high. Furthermore, we believe that seats sold for Citrix access are highly utilized and, therefore, count strongly on execution.

[↩ Return to Top](#)

#### Cautions

- Citrix supports full, tunneled network access but this capability has been less appealing for IPsec replacements because of the company's greater visibility and track record with an application delivery focus.
- Citrix needs to improve the base coverage and the ability for users to customize host checking and anti-malware defense components of its on-demand security tools as well as to make third-party integration more visible to customers.
- Citrix needs to demonstrate compelling application delivery on wireless handheld devices using the in-house technologies it has acquired during the past several years.

[↩ Return to Top](#)

## F5

#### Strengths

- F5's platforms are mature, reliable and scalable. F5 has delivered on planned expansion for integration and interoperability between Firepass and BigIP series products.
- Its Visual Policy Editor makes access control setups easy for administrators.
- Its very successful related business lines for acceleration and load balancing enhance company viability.
- Its iRules scripting system enables complex gateway operations to be programmed that might otherwise require custom coding, and is superior to proxy programming services in other products in the market.
- Several global providers use F5's products to deliver remote-access services.

[↩ Return to Top](#)

#### Cautions

- F5 is cited as a competitive threat by less than half of the vendors in this review, down from three quarters in 2007. Gartner client VPN inquiries occasionally reference F5.
- Its revenue in the line of business is more on a par with top-placing visionary players. Seat sales are impressive but behind the multiyear bar set by Juniper Networks and Citrix, and the steep challenge tendered by Cisco.

[↩ Return to Top](#)

## Juniper Networks

#### Strengths

- Juniper Networks delivers solid multiyear performance with strong sales and revenue in SSL VPNs and in IPsec. In general, Juniper can sell more product at higher incremental revenue than any other company in the market.
- Juniper is the No. 1 competitive threat cited by all other peer vendors, in fact, all 11 other ranked vendors named Juniper as a threat.
- The company appears on most shortlists discussed in Gartner client inquiries.
- Year after year, Juniper's products earn a high satisfaction rating and few complaints, given its high degree of market penetration.
- All its platforms have been CC EAL 2-certified since 2005.

[↩ Return to Top](#)

#### Cautions

- Juniper's stated list prices are among the highest in the market, but negotiable.
- Juniper's value proposition on a vision scale is excellent, but somewhat less compelling in terms of application delivery than Citrix and Microsoft.
- In 2008, estimated seat sales from Citrix and Cisco are outperforming Juniper.

[↩ Return to Top](#)

## Microsoft

#### Strengths

- Microsoft's merging of Internet Security and Acceleration Server, and the former Whale SSL VPN,

created an excellent new product, the Intelligent Application Gateway (IAG), with optimizations and strong sell-through for the Microsoft SharePoint Server.

- Its platforms and pricing are attractive for small to large enterprises, and are sold with Forefront Security.
- Coupled with SharePoint and Windows Terminal Services, Microsoft has a strong single-source solution for application and network access.

[↩ Return to Top](#)

#### Cautions

- Microsoft continues to suffer from fragmented, VPN developments on different platforms and in different product groups. Microsoft has a long-term vision for a converged VPN architecture, but buyers should expect to wait another year for a common architecture to be offered consistently across PCs and handhelds, with third-party support for non-Windows platforms.
- Endpoint security protection functions are good, including endpoint configuration detection and attachment wipers, but could be expanded. Microsoft recommends using Terminal Services application delivery to improve isolation, but this does not resolve all potential exposures from client-side malicious code. However, for many clients, the solution will be good enough, or third-party tools can be integrated.
- Support on non-Windows platforms was limited during the survey period, but additional support for Macintosh, Linux and Firefox included in Service Pack 2 needs to be expanded. Better SSL VPN support for handheld devices would also be desirable.

[↩ Return to Top](#)

### NeoAccel

#### Strengths

- Its gateway is available in a hardware appliance or as software (virtual appliance under VMware ESX Server).
- NeoAccel is attracting a good balance of new customers worldwide for IPsec replacements.
- Its increasing emphasis on OEM agreements and distribution, instead of direct sales, makes better use of resources.

[↩ Return to Top](#)

#### Cautions

- NeoAccel is the newest entry we track in a mature, consolidating market.
- Sales revenue and seat shares are growing, but are still below the median and far below the average for 2007 and 2008.
- The company could be an attractive acquisition target.

[↩ Return to Top](#)

### Nortel

#### Strengths

- Nortel is a large, global company with extensive worldwide support.
- The company offers products that converge IPsec/SSL clients, giving the user one experience, regardless of access mode. Nortel's TunnelGuard endpoint security has been adapted for SSL and is compatible across SSL VPNs and IPsec VPNs.
- Among major vendors, Nortel's seat pricing in large quantities is the second-lowest, after Cisco.
- Acceleration is standard/included on all models and platforms.
- In August 2008, Nortel released "Secure Portable Office," a trusted portable personality with an embedded VPN client, WAN optimizations and virtual desktop designed to run on an Aladdin Universal Service Bus (USB) flash memory device.

[↩ Return to Top](#)

#### Cautions

- Nortel's SSL market growth is less than expected for a major networking vendor with a strong reputation in IPsec VPNs. Sales for 2007 and first half 2008 are below median and far below average. Revenue is also below average. The company's outstanding global reach and sound base of technology have not made it disruptive to other vendors in the market.
- Gartner clients inquiring about SSL VPNs are likely to consider a separate vendor for SSL, even if they use IPsec VPNs and other products from Nortel.
- Nortel's 3Q08 results revealed a 14% year-over-year decline in revenue. There is also a plan to reduce staff. Some business units may become acquisition targets (see "Nortel's 3Q08 Results Focus Attention on Its Viability").

[↩ Return to Top](#)

### PortWise

#### Strengths

- PortWise is a stable vendor with steady sales and a strongly growing OEM business. Until recently, PortWise was the only tracked vendor with a virtual appliance and integrated, strong authentication for mobile devices.

- Sixty percent of buyers purchase PortWise's strong authentication to supplement the VPN.
- The gateway is software-based and is available as a VMware software appliance.
- PortWise has extensive experience in delivering secure services and applications to handheld wireless devices, including a long track record with sensitive applications, including retail banking and credit card terminals, and industrial applications such as vehicle management.

[↩ Return to Top](#)

#### Cautions

- Gartner clients have been unlikely to report PortWise as a shortlist candidate; however, verified case studies are of high quality.
- Its 2007 and 2008 reported seat sales are viable, but relatively low among surveyed vendors. PortWise would make a good acquisition target.

[↩ Return to Top](#)

### SonicWALL

#### Strengths

- A year after the acquisition of Aventail, SonicWALL has done an excellent job of integrating Aventail's mind-set, vision and road map with SonicWALL's hardware and distribution experience. Transition issues are resolved and clients are reporting favorable experiences.
- SonicWALL is delivering on time with its road map, low cost, highly scalable and green architectures for all of its products.
- Its Windows Mobile support has been available for 12 months and handheld optimization technologies are on the road map.

[↩ Return to Top](#)

#### Cautions

- SonicWALL needs to step out from behind its channels and compete more aggressively for "mind share" against its competitors. The company's greatest accolades seem to get published in reseller magazines that are not generally read by buyers.
- During the year of assimilation of Aventail, several managed service providers signed up to use competing vendors as alternatives or replacements.
- FIPS 140 certification will not be available until 2009. Most vendors in this market offer some degree of certification.
- Its original series of lower-end appliances directly support SMS one-time passwords. This capability should be expanded to the entire product line.

[↩ Return to Top](#)

*The Magic Quadrant is copyrighted 11 December 2008 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.*

*© 2008 Gartner, Inc. and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner's research may discuss legal issues related to the information technology business, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice.*