

2005 Best-in-Class SSL VPN Vendor Award

2005

FROST & SULLIVAN

Best-in-Class
SSL VPN Vendor Award

AWARD RECIPIENT: ARRAY NETWORKS

In a recent SSL VPN research study, Stratcast Partners (a Division of Frost & Sullivan) selected Array Networks as a 2005 Best-in-Class SSL VPN Vendor Award recipient for its comprehensive resource gateway SSL VPN solution. Array Networks has been able to attract enterprises with its value of tight integration, unmatched performance, administration efficiencies, security event correlation, consolidation of network and security devices, and reduced number of vendor products required due to its single-vendor solution.

Array Networks is a technology leader in high-performance, secure universal access solutions. The company provides fast and scalable SSL VPN products. Customers include financial institutions, healthcare organizations, telecommunications companies, large enterprises, government agencies, universities and service providers.

This Best-In-Class SSL VPN Vendor Award was bestowed on a small subset of SSL VPN vendors that have successfully integrated comprehensive feature sets in each functional category of connectivity, security, and performance. While Array Networks is the only smaller, private company among the five companies best positioned to deliver a comprehensive resource gateway SSL VPN solution, Stratcast Partners outlines in the report that Array's market progress with customers and partners demonstrate that its purpose-built, high-octane platform is second to none in supporting all three functionality categories simultaneously.

Array Networks SPX Series SSL VPN solution exercises significant control over the traffic between end users and resources. Such monitoring can help detect and block zero-hour attacks (non-signature based), anomalous behavior, and - at the most discrete level - positive logic application firewalls to allow only specific end-user interactions with resources. Array's SSL VPN approach also offers optimized end-to-end performance between end users and backend resources. Array Networks aims to reliably replicate local area network (LAN)-based end-user experiences, when connections do not originate on-site, across a broad range of applications and resources.

Best-in-Class Selection

In this report section, we provide our selection of vendors that are best positioned to thrive as comprehensive Resource Gateway solution providers. While it is our belief that the market will eventually migrate to Resource Gateway solutions

that offer comprehensive feature sets in each of the functional categories - connectivity, security, and performance - the market reality is that only a portion of the vendors reviewed have the means to integrate all of the parts together from within their own organization. Furthermore, even if all the functional categories are assembled into a single solution, enterprise adoption rates will vary for several legitimate reasons. Those reasons include:

- Concern about a creating single point of failure or performance bottleneck.
- Reluctance to retire existing network and security devices that adequately meet current requirements and are not fully depreciated.
- Enterprise desire to retain flexibility in vendor selection and to maintain vendor diversity.

Nevertheless, we do expect that there will be growing market interest for comprehensive Resource Gateways by those enterprises that are attracted to the value of tight integration, administration efficiencies, security event correlation, consolidation of network and security devices, and fewer vendor relationships a single-vendor solution can potentially offer. Certainly, this is not a new market phenomenon as device consolidation in the security industry has a lengthy history. Relevant examples include the collapsing of separate VPN and firewall technologies onto a single device followed by the layering of security inspection technologies (e.g., IDS/IPS, URL filtering, anti-virus).

In essence, security devices are continuously adapting to defend against an evolving threat environment. For the same reasons that multiple security technologies are combined into a single solution, we believe traffic management and application acceleration technologies will be additional functional overlays. By virtue of its location between end-users and resources, Resource Gateways occupy a logical juncture (i.e., at a point of traffic aggregation and where encryption/decryption occurs) to deliver these technologies.



2005 Best-in-Class SSL VPN Vendor Award

2005

FROST & SULLIVAN

Best-in-Class
SSL VPN Vendor Award

The distinction between lower and upper tier functionality is described in the below figure. In addition, we believe for long-run competitiveness that the vendor will need to “own” the technology they are delivering to the market through in-house development, acquisitions, or OEM technology licenses. Technology partner integration, in our view, will only be competitively viable in the near-term (12 - 18 months) while the vendors that have direct ownership of the technologies develop the platforms capable of delivering on all three functional categories.

Conclusion

Array Networks has delivered product advances that have simultaneously delivered higher levels of functional sophistication and improved administrative and user friendliness. For these reasons, Array Networks is the deserving recipient of the Best-in-Class SSL VPN Vendor Award.

Functionality Tiers of Resource Gateways

Functional Category	Lower Tier	Upper Tier
Connectivity	Technology limitations require multiple access solutions to be used due to differences in resource types, accessing locations, and endpoint platforms.	Deliver on the concept of a Universal VPN in which access to any resource, from any location, with any endpoint platform is reliably supported and with limited end-user and administrator involvement. Implicit with this concept is that enterprise security and resource use policies dictate access rights, not technology.
Security	Granular access control inclusive of endpoint security policy enforcement (i.e., assessing the security state of the endpoint device as a factor in assigning resource access privileges).	Control exercised over the traffic between end-users and resources to detect and block zero-hour attacks (i.e., non-signature based), anomalous behavior, and, at the most discrete level, positive logic application firewalls to only allow specific end-user interactions with resources.
Performance	Optimized gateway performance (scalability, high throughput, and low and consistent latency levels).	Optimized end-to-end performance from end-user through to backend resources and vice versa. Ultimate goal is to reliably replicate on-site (LAN-based) end-user experiences when connections do not originate on-site across a broad range of applications and resources.

For more information, contact:

Array Networks
408.240.8700
www.arraynetworks.com

Frost & Sullivan
210.247.2450
www.frost.com