

IDC Viewpoint



Viewpoint: Why Security Appliances?

October 2003 Doc #VWP000180

Charles J. Kolodgy
Research Director, Security Products

IDC predicts that by 2007, 80% of all security solutions will be delivered via a dedicated security appliance. Security appliances are defined as a combination of hardware, software, and networking technologies whose primary function is to perform a specific or multiple security functions. The security appliance consists of hardware with a hardened operating system (OS), a limited applications set, and no user software installation. Security appliances may also include other features such as security management, policy management, quality of service, load balancing, high availability, and bandwidth management.

Security appliances originally were restricted to firewall/VPN functions, but now there are appliances available for almost all security functions, including but not limited to intrusion detection and prevention, antivirus, secure content management, authentication, vulnerability assessment, and security event management. The growth of appliances as the platform for security software delivery is amazing, but the question is why?

Security appliances have been popular because they can solve pain points for customers, managed service providers, resellers, and product vendors.

Benefits to Customers

- Turnkey solution: Security appliances are plug-and-play and take very little technical knowledge to install. By using a Web browser for device management, end users can easily manage remote locations.
- Total cost of ownership: Software solutions can quickly drain IT resources with prolonged installation, education, and maintenance costs — even more so when the costs of purchasing the hardware to load it on are factored in.
- Performance: Security appliances have a specific level of imbedded performance with customizable features based on hardware/operating system/database packaging, while software solutions depend on whatever hardware configuration the reseller or customer uses.
- No operating system or database licensing: Customers do not need to license an operating system or database when using a security appliance, as it is an integrated component of the solution.
- Security hardened: Security appliances are hardened, which negates hacks and eliminates other applications from running on the same appliance.

Benefits to Service Providers and Resellers

- Additional sales opportunities: Service providers and resellers can up-sell additional security features to existing customers.
- Reduced maintenance costs: The appliance model can reduce truck rolls because troubleshooting can be done remotely and failed units can be swapped out easily by contacting only one source.
- Service offering opportunities: Through the use of appliances, services can be built around appliances.

Benefits to Product Vendors

- Additional opportunities: By providing their products via security appliances, either on their own or in partnership, product vendors can expand their opportunities by expanding the number of resellers willing to carry the products or by adding security features to existing appliances.
- Performance guarantee: Product providers can ensure that their products will meet customer needs by providing known performance metrics.
- Operating system neutrality: With appliances, software vendors can limit what operating systems they will support, instead of needing to produce a product version for all enterprise operating systems and databases.
- Meet customer need: By providing appliances and sometimes software, product vendors can satisfy customer needs with multiple options.

In summary, security appliances are popular because they offer substantial advantages in performance, convenience, and choice to customers, resellers, and product vendors. IDC would expect those vendors that have already gone the appliance route will have a material advantage over competitors that are not pursuing an appliance strategy.