



Charles Kolodgy
Research Director, Security Products

Security Appliances: New Technologies, New Business Partnerships Benefit Enterprise Customers

September 2007

In the past few years, companies have embraced security appliances as a way of protecting their networks from unauthorized use. Over time, security appliance vendors have offered more functionality, and customers have become increasingly dependent on these appliances to protect assets and to enable business transactions. Integrated security appliances address customer concerns regarding cost, manageability, and stability. Although security appliances are still in their infancy, as virtualization technology is adopted, they will offer more functionality, options, and ease of use. Software companies adopting the appliance model will increasingly look to hardware vendors for total life-cycle support and value-added services to ensure their brand loyalty, keep down reverse supply chain costs, and maintain high levels of seamless customer experience.

The following questions were posed by Dell Inc. to Charles Kolodgy, research director of IDC's Security Products service, on behalf of Dell's enterprise customers.

Q. Could you define the term "dedicated security appliance" and describe the role this product plays in a company's overall security strategy?

A. IDC defines a security appliance as a combination of hardware, software, and networking technologies whose primary purpose is to perform one or more security functions. The security appliance consists of hardware with a hardened operating system (OS), a limited application set, and vendor-installed software sold as a single bundle. Security appliances may include features such as security management, policy management, quality of service, load balancing, high availability, and bandwidth management.

Originally, security appliances were restricted to firewall/VPN functions, simply protecting the company network from unauthorized use. Over time, appliances have become available for many more security functions (e.g., intrusion detection and prevention, antivirus, secure content management, authentication, vulnerability assessment, and security event management), enabling greater protection from hackers and from viruses that might be introduced by mobile worker computers. More importantly, these devices have become essential components of the business model in many enterprises, protecting financial transactions and enforcing service agreements.

Q. Security appliances have experienced meteoric growth, with threat management appliances having grown over 800% since 1999. Why have security appliances become so popular, and why will they remain popular?

A. The worldwide security appliance market has become a powerhouse, growing rapidly even when the economy was down. Security appliances have been popular because they can solve several important pain points and offer distinct advantages for customers, software companies, and hardware vendors.

Benefits to customers include performance because security appliances have a specific level of performance while software solutions depend on whatever hardware configuration the reseller or customer uses; minimal installation and configuration because most security appliances are plug and play and require very little technical knowledge to install and manage; no operating system licensing; and hardened security against hacking, thus freeing the customers from this concern.

The benefits to software companies (appliance resellers) include upsell opportunities to existing customers because of additional security features and improved customer experience; faster time to market and reduced development and test time compared with traditional software delivery; ability to enhance the brand with distinctive customized hardware options and features; and reduced overall maintenance costs because hardware is deployed on a controlled platform, troubleshooting can be done remotely, and failed units can be easily swapped out or serviced in-field.

The benefits to hardware vendors include a performance guarantee that their appliance will meet customer needs by providing known performance metrics and operating system neutrality because, with appliances, software vendors can limit what operating systems they'll support instead of needing to produce a product version for all enterprise operating systems. Also, appliances can meet customer needs for multiple options.

Additionally, the marriage of hardware and vendor-installed software offers convenience and ease of installation for enterprise organizations seeking threat management solutions. These devices are designed to be easy to configure "out of the box," without needing the extensive integration required by some comparable software packages. Buyers know that faulty units will be easily serviced or replaced by the appliance reseller, saving time that might be spent on a technical support phone line or having to manage the technical issue in-house. The preconfigured devices are optimized for performance, are hardened against hackers, and are more cost-effective than solutions that must include fully functional operating systems.

Large enterprises value the centralized management capability that many of these security appliances offer. Many vendors have designed into their products advanced enterprise features, including quality of service (QoS), load balancing, high availability, clustering, and bandwidth management, as well as security and policy management. The presence of so many features allows companies to roll out comprehensive security measures quickly. This can be a huge advantage for companies seeking to add new network bandwidth and applications.

Q. So appliances marry hardware and software into one package. Is that all there is to it?

A. As in any marriage, choosing the right hardware partner is critical to success. A security software company needs to partner with a hardware company that provides the right mix of integration, fulfillment, and support services.

The devices themselves are evolving to deliver more complex functionality. This changes the hardware configuration (i.e., PCI-E cards, ports) as well as the software. The new functionality increases not only the critical value of the appliance to the end customer but also the complexity of the solution. As a result, the end customer, especially in the case of an enterprise customer, is likely to require more support.

Because security software vendors in many cases are partnering with hardware companies that can provide some of this support, the partnership becomes an important part of the solution. The enterprise customer will want a vendor it can trust — one that has a sound understanding of the role these devices play in the modern enterprise, can provide customized solutions without impacting quality, and can provide support from design through execution, as well as life-cycle management and support. This would enable the security software vendor to focus on core competencies, leaving traditional fulfillment, hardware design and quality issues, and hardware support to the hardware vendor.

Q. A few years ago, you predicted that, by 2007, 80% of all network security solutions would be delivered via a dedicated security appliance. How do you feel about that prediction now?

A. That prediction has been very solid. Security appliances, including what they enable, dominate the security landscape. The key to security appliances isn't just what the appliance does when you buy it, but the continuing services running on the appliance. Most security solutions require constant updates to keep up with changing threats. To do that requires software subscriptions to update the security signatures. This is the real value provided by appliances, and why it is correct to say that 80% of network security solutions are delivered via a dedicated security appliance.

As mentioned, appliances were generally restricted to firewall and VPN functions, but now almost all security functions can be purchased on an appliance. Even solutions that rely on host software agents utilize appliances as management consoles. Products continue to evolve to offer more functionality, features, and services. The success of threat management appliances affects areas that were thought to be immune to this trend, such as secure content management (SCM) and security and vulnerability management (SVM). The reality is that any type of software can benefit from being packaged in an appliance. New technologies enable new services, which, in turn, require new security solutions. The market is still growing. Worldwide revenue for all security appliances was \$5.2 billion in 2006 and is forecast to grow to \$10.4 billion in 2011, a compound annual growth rate (CAGR) of 15%.

The success of security appliances is leading nonsecurity services such as search, database, and video on demand to look at the appliance model as well. We anticipate that this model will translate very well for a broad base of software applications as industry leaders and upstarts alike take advantage of the highly customizable and flexible appliance programs already set in place by the security software industry and a variety of key hardware vendors.

Q. As the person who coined the term "unified threat management," or UTM, obviously you're close to this market. What new trends will be driving this market in the next few years?

A. UTM appliances, which include multiple security features integrated into one device, were the first round of integrated appliances. Because UTM appliances address customers' demands for fewer network devices and improved manageability, demand will increase. The real value of a UTM appliance is that it allows customers choice in how they want to deploy their security services, but they get the benefit of consistent device management.

Interestingly, virtualization technology is becoming an enabler of UTM appliances and other integrated devices. Once the majority of installed servers include an installed hypervisor or virtual machine layer, the infrastructure is in place to support multiple operating systems, each carrying one or more application workloads. This same many-to-one multiplexing of operating system images aboard servers also makes it possible to locate software appliance functionality aboard these same servers, leveraging otherwise unused capacity.

The future of UTM may not be a combination of products that vendors decide to include; it may be a mix of software appliances that customers choose to fit their needs. This will allow vendors to sell the products piecemeal or as a package and still have a single management console. It also may be possible, with the right management tools, for customers to create their own UTM appliances with best-of-breed point solutions from several different vendors. The only limitation on what a customer can install is the limitation of the processing power and I/O throughput of the infrastructure.

Overall, virtualization as applied to the hardware appliance market is still somewhat murky, with potential upsides and drawbacks. For example, virtualization may ease patching for software updates, facilitate load balancing and failover, and mitigate some of the challenges related to hardware platform changes. However the trade-offs are not to be overlooked in terms of potential increased costs in licensing, added layers of software required to validate and test the application, which could sacrifice performance, and the custom hardware configurations that certain applications rely on today as part of their hardware appliance solution.

Also, support for virtualized platforms is an issue yet to be resolved. The evolution of virtual technologies still has many years to play out, but IDC anticipates that virtualization will eventually marry well with turnkey hardware appliance solutions. We can envision a time when virtualized appliances facilitate the pushing of higher-end functionality to a lower-cost and expanded customer base. Then, when added performance, functionality, and security certification are required, customers will be able to upgrade their dedicated hardware appliance solutions.

ABOUT THIS ANALYST

Charles Kolodgy is a research director for IDC's Security Products service. In this role, he executes primary research projects and analyzes markets for both vendors and user customers. Mr. Kolodgy's responsibilities within the Security Products service include both hardware and software security products.

ABOUT THIS PUBLICATION

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests, contact the GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC.

For more information on IDC, visit www.idc.com. For more information on IDC GMS, visit www.idc.com/gms.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com