IDC
Analyze the Future

I D C A N A L Y S T C O N N E C T I O N

Jon Crotty
Research Analyst, Security Products and Services

Virtual Security Appliances on the Rise

March 2010

Security is a critical component in the growing ecosystem surrounding virtualization. Virtual security appliances (VSAs) play a vital role in fulfilling IT expectations today, and will continue to do so in the future — an unusual situation for a relatively new technology. Companies of all sizes and across all industries are looking toward VSAs to address business and security needs in the virtual world.

The following questions were posed by Trend Micro to Jon Crotty, a Research Analyst with IDC's Security Products and Services group, on behalf of Trend Micro's customers.

Q. What are virtual security appliances and why are they growing in importance?

A. IDC defines virtual security appliances (VSAs) as software products that integrate an operating system and layered security-centric software into an easily managed composite package that can be deployed aboard industry-standard client or server hardware, either on a virtual machine or directly on the hardware. A virtual security appliance is capable of being installed directly on hardware, but in the vast majority of the cases will be delivered inside a virtual machine on a hypervisor layer. Ease of management, disaster recovery, simple integration with current infrastructure, ease of deployment and administration, and high availability are all helping drive the demand for VSAs.

A recent IDC study on virtual security appliances shows that over 50% of North American organizations are currently deploying or have deployed VSAs. Furthermore, 77% of IT professionals say they now have monies set aside specifically for virtual security appliances. IDC's survey data shows a noticeably higher percentage of virtual security appliances fully deployed among small to medium-sized companies, as compared to large companies.

We do expect to see rapid adoption in larger organizations where buying cycles typically tend to be more drawn out. Companies of all sizes and across all industries are looking toward virtual security appliances to address business and security needs. These appliances play a vital role in fulfilling IT expectations, and will continue to do so in the future. This market acceleration is an unusual situation for a relatively new technology. However, it's easily understandable when you look at how these products play such an important role in things such as Green IT, datacenter consolidation, and improved security.

Q. What will the emergence of the virtual security appliance market do to the traditional security hardware market?

A. We are still in the very early stages of virtual security appliances being fully deployed. The traditional hardware security market (Firewall, IPS, UTM, VPN, etc.) will continue to grow, but at a slower rate compared to virtual security appliances. Moreover, certain VSA submarkets, such as gateway content filtering, are seeing very fast rates of deployment.

Web and messaging security appliances, specifically, focus on content security, so these systems are not saddled with the networking challenges of firewalls and UTMs. Because Web and messaging appliances are not dependent on network security, their independence drives a rapid adoption of virtual Web and messaging security appliances. When replacement cycles are reached, many IT professionals are opting to fully deploy Web and messaging security functions in the virtual appliance form factor.

What's interesting is that virtual security appliances are not really a new phenomenon, as testing environments have used VSAs for many years. However, rising virtual security appliance usage in production environments is proving to be a belly punch for traditional hardware security vendors. They did not expect high customer interest that would result in rapid growth.

Other physical security appliance pain points, such as high total cost of ownership (TCO), reusability, separate warranty contracts, and replacement cycles, are driving many IT professionals towards virtual security appliances. Recent IDC research shows that 83% of IT professionals who have deployed both physical and virtual security appliances are very satisfied with the virtual security appliances. These results have been quite consistent across all company sizes.

Q. What are the key benefits of virtual security appliances?

A. In many cases, these products can give a hard elbow to traditional hardware appliances. They are clearly a boon for Green IT, datacenter consolidation, and overall virtualization initiatives. They increase IT flexibility in terms of how and where applications run and improve business continuity through more efficient automation such as provisioning, load balancing, failover, and disaster recovery practices. Hardware appliance vendors market newer products as "green" by highlighting faster and more powerful boxes, whereas virtual appliances give back real estate by literally shrinking the datacenter footprint. This visual transformation is stunning.

The TCO benefits of virtual appliances are very impressive when considering things such as application deployment, redundant capacity, and proprietary hardware. Virtual appliances have always been leveraged for safe testing environments. Resource allocation for operational segmentation becomes very flexible when virtual security appliances are introduced to a security architecture. Virtual security appliances give IT professionals the flexibility and the ability to segment people or data more easily. There is a clear benefit in terms of how and where applications run. The same best practices in the physical security world can also be used in the virtual environment. Patching, monitoring, maintenance, and management can be easier and less consumptive of time and resources.

Recent IDC research shows that 62% of IT professionals see virtual security appliances as a way to directly deal with flexibility and scalability concerns in their security infrastructure. Furthermore, 52% of IT professionals see reducing floor space, as well as power and cooling costs, as key benefits. In addition to the issues mentioned, we believe virtual security appliances are a turn in the right direction against hardware appliance sprawl.

Q. Why are Web security and messaging security currently two of the most popular applications for virtual security appliances?

A. IDC's recent Virtual Security Appliances Survey showed that the top two types of virtual security appliances currently in use are for Web security and messaging security. We believe the high rate of adoption for virtual security appliances is synergistic with current server virtualization strategies, which is a natural reaction to the proliferation of too many small appliances. This is something IDC calls "appliance fatigue." There is building frustration from IT managers who struggle to manage the growing number of hardware boxes deployed at the gateway (Firewall, IPS, VPN, Messaging Security, Web Security, UTM, etc.).

In the messaging security area, it's become even more of a burden. As the pure volume of spam continues to rise at an alarming rate, organizations have been forced to deploy additional boxes just to keep pace with email traffic. This has created both a management and cost nightmare, and is a key driver behind the interest in virtual security appliances. IDC believes that, as organizations look for ways to cut hardware costs and simplify IT management, virtual appliances will increasingly become a very attractive platform of choice for customers looking to save money in today's uncertain economic climate.

Organizations are clearly excited about the benefits of VSAs. However, they should keep some things in mind before adopting. IDC believes customers will not sacrifice security effectiveness in exchange for the benefits of virtualization when purchasing a virtual appliance from a leading security vendor. The virtual appliance should have all of the bells and whistles of best-of-breed hardware and traditional software solutions in the market today. These include bi-directional filtering capabilities (inbound for spam and viruses, and outbound for data-loss prevention), reputation services, and advanced malware and spam techniques.

Q. What role will virtual security appliances play in the evolving datacenter architecture and cloud computing?

A. According to IDC research, security is the number one customer impediment to cloud implementations. Security represents the underlying prerequisite to catalyze large-scale deployment of virtualization and cloud adoption. Looking deeper into this issue, IDC discovered that IT wants to help alleviate user concerns, but datacenters supporting private and public cloud providers struggle with their own issues.

Security and associated system administration challenges include portability of virtual machines, provisioning of security applications, load balancing, capacity planning, failover, high availability, and movement between public and private clouds. In the last instance, customers want the flexibility to discontinue a public cloud relationship that fails to meet their needs and move their data and applications back to a private cloud.

IDC believes that virtual security appliances can help solve these problems. These products can be moved between public and private clouds, so the same internal and external compliance policies can be maintained regardless of physical location. Virtual security appliances also offer major benefits relative to load balancing, capacity planning, uptime, and variable service requirements. In line with existing server virtualization initiatives, virtual security appliances maximize computing resources. Because virtual security appliances were designed for cloud infrastructure, service providers are deploying them in their datacenter to secure hosted applications and maximize applications performance.

ABOUT THIS ANALYST

Jon Crotty is a research analyst within IDC's Security Products and Services group. He conducts in-depth primary research and is responsible for analyzing and forecasting a variety of evolving security markets. Mr. Crotty provides critical market intelligence to technology vendors, IT professionals, and the financial community. His areas of expertise include, but are not limited to: EndPoint Security, Consumer Security, Network Security, Messaging Security and Web Security.