IDC Analyze the Future

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

Charles Kolodgy
Research Vice President, Security Products

Server Security for Today's Datacenters

February 2012

The endpoint security market encompasses products that are designed to protect endpoints from attack or to directly protect information residing on endpoints. Server security is a subset of this market. In general, endpoint security is the final line of defense in the ongoing battle with malware. Some form of endpoint security (e.g., antivirus, threat management, encryption, or a suite with multiple solutions) resides on the vast majority of machines. With more endpoints being mobile (which now includes virtual servers residing at remote datacenters), and thus out of the direct control of the enterprise, endpoint security requirements increase. The endpoint cannot rely solely on the network security infrastructure because many times the endpoint will be connecting to the Internet via an untrusted network connection. The information that can be acquired from endpoints, including clients and servers, has kept corporations buying endpoint security at a record pace. In 2010, the endpoint security market was $7.2 billion. IDC expects this market to grow at a compound annual growth rate (CAGR) of 8.1% from 2010 to 2015, reaching total revenue of $10.6 billion in 2015.

The following questions were posed by Trend Micro to Charles Kolodgy, research vice president of IDC's Security Products service, on behalf of Trend Micro's customers.

Q. Why is server security different from other forms of endpoint security?

A. Endpoints are divided into two general categories: clients and servers. The client is a standalone computer that can perform multiple tasks. Servers, meanwhile, generally have more computing power, are network resources, and feed data to other devices (meaning they serve content). Servers have many functions. They receive data or input from network-connected devices, process what is required, and return output. A quick way to look at these two endpoints is that a client performs multiple tasks for one and a server performs a singular task for many. Because a server is providing services for many, its value to an organization is generally higher than that of a single client. A server will have access to considerably more data than a single client because it will have files or host email accounts from everyone it serves. A server will be exposed to many more threats than a client because a server connects to so many other endpoints and because it is a higher-value target than a single endpoint. This is the crux of the difference between server security and other forms of endpoint security; server security must be more robust than client endpoint security because it is protecting a higher-value target. Another distinguishing factor associated with servers is that they run a wider range of operating systems (Windows, Unix, and Linux). With the emergence of server virtualization, there is also a need to provide security for virtual machines (VMs) in addition to single-device servers.

Q. How do you define the requirements of server security?

A. Server security, like all endpoint security, consists of key protection functions including antimalware, firewall, and a host intrusion prevention system (HIPS). Other server security functions include, but aren't limited to, vulnerability assessment, application control, and file integrity monitoring. However, the relative importance of these functions is different for servers.

For a server, intrusion prevention is the key security tool. It is designed to maintain the integrity of the server. A HIPS protects the server's operating system to ensure that the system does not run malicious software that can compromise the business applications and data on the server. A HIPS is designed to prevent an attacker from gaining control of the server's operating system. Advanced HIPS programs can also provide "virtual patching" by preventing attacks that target known vulnerabilities even when the vulnerability has not yet been closed. A HIPS is much more effective on servers than on client devices because a HIPS can be configured to protect the specific task of the server. Because a client can perform so many functions, it is much more difficult to have a single program that can lock those functions at the operating system level.

The firewall function is second to the HIPS function because of the high number of network connections a server receives; the firewall must ensure that the connections are within the server's policy. Antimalware is the third line of defense. When antimalware is coupled with a strong HIPS, malware should not be able to compromise the server's operating system. The other security options vary in importance based on server type and an organization's industry. For example, the Payment Card Industry Data Security Standard (PCI DSS) applies to companies that accept funds through payment cards and calls for file integrity monitoring (PCI 10.5.5 and PCI 11.5) as part of its security standards.

One of the trends for all endpoint security is the rise of integrated security suites that combine different security technologies into one program. Organizations are moving to suites because they want to deal with fewer vendors. Some suites also provide security on a single security platform with a single, integrated agent, which is easier to install and manage while being able to match the capabilities of individual standalone products.

Q. How do virtualization and cloud computing impact server security?

A. More and more organizations are using cloud-based infrastructures to host their applications, generally in the form of virtual servers. This only expands the issues associated with server security. Using a cloud-based infrastructure that isn't in your complete control and virtual servers, which can be active or dormant, makes it more difficult to ensure full protection. Server security, in many cases, then becomes a management issue. Thus, the number 1 requirement for cloud-based virtual server security is to have a specialized security framework with a complete set of management tools that are designed to protect the dynamic and shared resource environment of virtual and cloud infrastructure. These tools need to be able to identify what servers are running, the security posture of the servers, and alert an organization when security isn't up to standard.

In addition, when organizations utilize the cloud, they need to ensure that their data is safe. For this data protection component, people will turn to the server because it is where the data is stored and processed. For cloud-based deployments, data protection — be it encryption or data leak protection — is required. These data protection capabilities must also be managed.

This brings us back to the key security question, "Can I ensure that I have the protections I require in this environment?" The same protection functions that are required (such as HIPS, firewall, antimalware, and file integrity monitoring) to protect physical servers are required to protect virtual servers. However, it isn't as simple as dropping the existing server security on each virtual server. Yes, that can be done, but it isn't the best overall solution because having a full agent on each virtual server requires considerable management overhead. As already stated, management is a key requirement, so adding overhead would complicate this function. This can also result in some performance degradation if multiple machines perform antimalware scans at the same time. This can ultimately cause lower VM densities and lead to a lower ROI for virtualization efforts. The better solution is to have a virtual security appliance that resides between the hypervisor and the virtual machines. The virtual security appliance handles functions such as on-demand antimalware scans and other high-impact security operations, providing coordinated security with minimal impact on performance. Other functions at the virtual machine level can be handled by a combination of agentless and small client software.

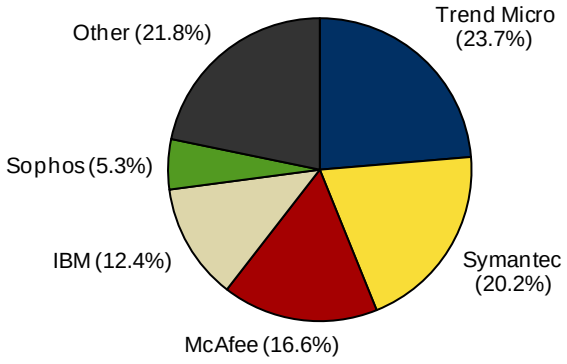
People are turning to cloud-based computing for performance and flexibility. Therefore, to improve security for those same reasons, organizations will need to supplement security for virtual servers with a cloud-based security service, such as file reputation or threat intelligence, that can prevent some malicious items from ever reaching the cloud-based virtual servers.

Q. What is the current revenue forecast for server security?

A. According to IDC, worldwide revenue for server security reached nearly $440 million in 2010; by 2015, revenue will approach $695 million. Figure 1 shows the 2010 worldwide corporate endpoint server security revenue share of the leading vendors.

Figure 1

Worldwide Corporate Endpoint Server Security Revenue Share by Vendor, 2010



Total = $439.2M

Source: IDC

Q. As the leader in server security market share, what is the key challenge that Trend Micro faces in the market for endpoint server security products?

A. The most difficult challenge within server security, as with any level of information security, is being able to address an increasingly sophisticated threat environment. There is a never-ending arms race between cyberattackers and cyberdefenders. The speed with which threats are increasing (hundreds of millions of malware variations) is making it increasingly difficult for signature-based antimalware to keep up. Signature databases are growing, thus impacting performance and making antimalware less accurate. Additionally, attackers are finding new ways to attack servers, discovering new vulnerabilities within applications and operating systems or new avenues of attack. They are using stealthy attack methods designed to evade existing defenses. The challenge for Trend Micro, as well as the industry, is to address this threat environment in a way that doesn't cripple server performance. To defend against these attacks requires new technology that reduces reaction time, thus making existing defenses more robust. Trend Micro has been addressing this challenge with its Smart Protection Network, which allows threats to be identified and eliminated in the cloud before they arrive at the endpoint, thus reducing the reliance on antimalware signatures at the endpoint level. For server-specific security, the company has been improving the application control and virtual patching functions within Deep Security to ensure that attacks can't gain a foothold on the server through a vulnerability. Deep Security is also provided as a server security platform with all technologies integrated into a single agent to offer additional performance and management benefits.

ABOUT THIS ANALYST

Charles Kolodgy is a research vice president for IDC's Security Products service. In this role, he executes primary research projects and analyzes markets for both vendors and user customers. Product areas of concentration include endpoint security, vulnerability assessment and management, and encryption. Research areas that cut across product markets include product certification, Web site security, threats, and security policy.

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

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