IDC TECHNOLOGY SPOTLIGHT

Server Security: Virtualization and Cloud Changes Everything

January 2016

Adapted from *Worldwide Endpoint Security Market Share, 2014: Success of Midsize Vendors by Elizabeth Corr, Robert Westervelt, Pete Lindstrom, and Christian Christiansen IDC #US40546915*

Sponsored by Trend Micro

This Technology Spotlight highlights how cloud computing and virtualization have transformed the way organizations should view server security. Although organizations have considerable interest in endpoint and perimeter network security, the modern data center, which includes physical, virtual, and often cloud servers, remains a valuable but neglected component of the infrastructure that must be protected. Importantly, most enterprises using the cloud will be deployed in a hybrid architecture for the foreseeable future, with workloads in the data center as well as the cloud. The key is that the security used to protect servers, regardless of where they are located, must be efficient in the context in which it is deployed in order to not degrade overall server performance. This paper defines what server security is, examines how and why the server security market is growing, and highlights the capabilities of Trend Micro in this strategically important area.

Datacenter and Server Security Overview

Security is at a major inflection point because of the changes taking place in the overall information technology (IT) environment. IT is evolving considerably as we move into what IDC calls the era of the 3rd Platform. Issues around the dynamic nature of datacenter environments, the speed of server and application performance and deployment, and the expanding usage of cloud computing, virtualization, and social media all make protection seem like a game of "whack-a-mole." Cybercriminals, using advanced tools, can pick and choose how and who they will attack. Given this environment, it's important to provide a strong level of security throughout an organization's infrastructure and beyond into the cloud.

The security used within the datacenter, primarily server security, has been evolving to protect virtualized server instances, regardless of whether they are physically located in an enterprise's datacenter or reside in a cloud-based environment. Technologies used to control the flow of traffic and prevent malicious activity have evolved to scan not only physical but also virtual environments. Additionally, the ability to segment Layer 7 traffic is much more important now than it was just a few years ago. The need for strong security, antimalware, intrusion protection, and vulnerability protection has been driving interest and innovation in datacenter security, especially for server security. IDC saw the server security market grow to over $800 million in 2014.

Server Security Defined

Servers are the workhorses of IT. They are, from a user perspective, the applications that fulfill requests for content or some other function sent by client computers — stationary or mobile. The server shares its resources with the clients by hosting applications that perform computational functions and store and retrieve data. Servers have various functions that include processing email, serving up Web pages, managing databases, saving files, and running applications.

Servers in a datacenter are closely interconnected, with one request from a client often needing to be processed by a number of servers. Servers used to be single-function hardware, but with virtualization technology, it's now possible to have hundreds of virtual servers on one piece of equipment by utilizing a hypervisor that manages the processing allocations among various servers. Many server farms now reside in hosted datacenters that are accessed using the Internet. Server security is designed to ensure that the clients making requests do not inject malware into a server, giving an outside source illicit access to the server's operating system or applications.

Server security solutions include all types of security functions — antimalware, endpoint firewall, host intrusion prevention, application control, file integrity monitoring, Web threat protection, and vulnerability containment. These functions are designed to maintain the health of servers, both physical and virtual.

Server security products protect server operating systems, helping to ensure that the systems are protected from external attacks and do not run malware or execute malicious code that can compromise the business applications and data on the servers. These products are generally more robust than desktop, laptop, and mobile device endpoint security and are available for a wide set of operating systems (e.g., Windows, Unix, and Linux). With the rise of virtualization server security, protection is now available for servers at both the host and hypervisor levels, giving organizations flexibility and control over how resources are utilized.

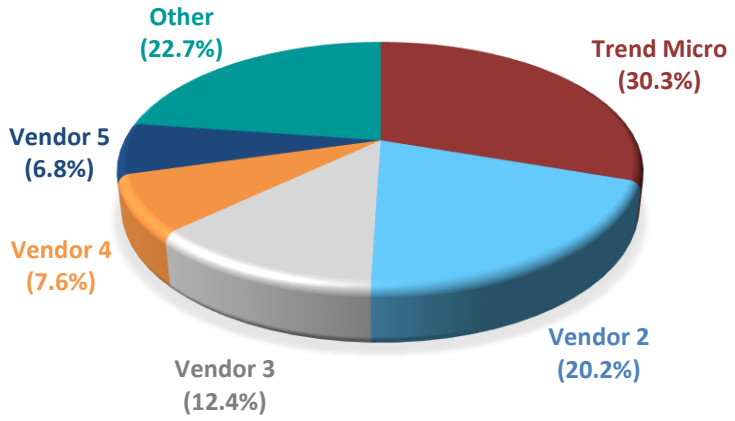
The Server Security Market

IDC considers server security to be a submarket of the endpoint security market. The market has experienced considerable growth over the years. IDC saw the server security market grow from $530 million in 2010 to $802 million in 2014, representing a combined annual growth rate of 8.9%. IDC forecasts that the market will near $1.0 billion by 2019. The CAGR over the 2014–2019 forecast period is 4.5%.

The market leader in server security each year since IDC started tracking the market has been Trend Micro. The company has not just maintained market leadership but also has increased its share of the market. In 2009, Trend Micro captured 23% of the server security segment, and by 2014 it had garnered over 30% share of the market. Figure 1 illustrates the market share of Trend Micro and its competitors in 2014. Figure 2 illustrates the market share shifts and overall market growth from 2009 to 2014.

FIGURE 1

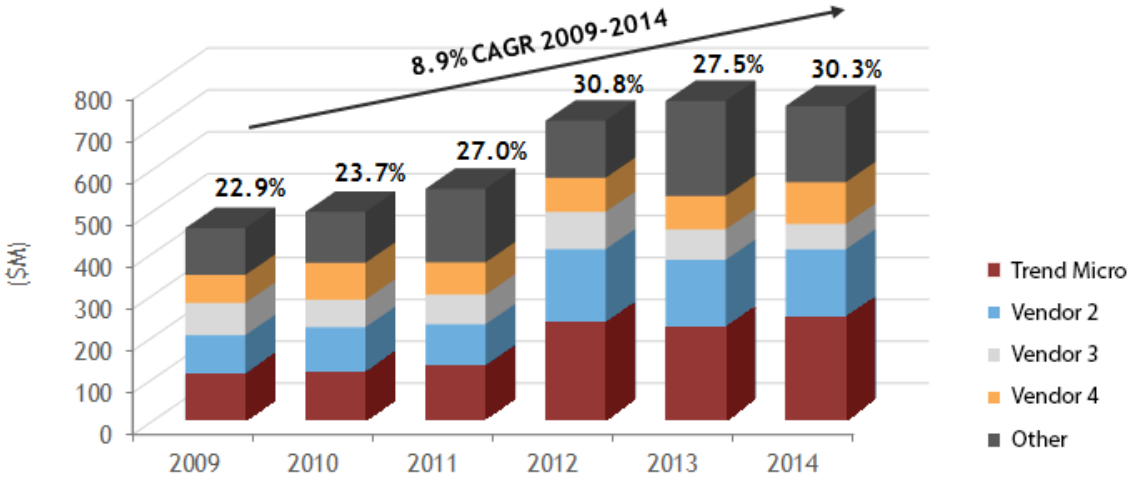
Worldwide Corporate Server Revenue share by Vendor, 2014



Source: IDC, 2016

FIGURE 2

2009-2014 Server Revenue ($M) with Shares



Source: IDC, 2016

Key Technology Trends in Server Security

Server security formerly consisted of two primary functions — antimalware and host intrusion protection. Antimalware applications were specifically designed to scan mail and file servers for malware to ensure that the server applications didn't pass on malicious payloads. Host intrusion protection was designed to harden the server's operating system against attack. These solutions also might have included a firewall to control a server's ports.

Although these components still exist, server security has been vastly improved with the consolidation of additional security functions. These new features don't just protect individual servers; by extension, they make the whole datacenter more robust against attack. Additional capabilities include application scanning, file integrity monitoring, Web threat protection, virtual patching, log inspection, and data protection. Server security has also been modernized to deal with specialized malware and with Web-borne threats that are often used to execute sophisticated targeted attacks.

Threats targeting endpoints—both desktops and servers—seem to be never-ending. The speed with which threats are growing makes it increasingly difficult for signature-based antimalware to keep up. Signature databases are likewise growing, thus potentially impacting performance and making antimalware less relevant as a single point of server security. Security products are moving to rely less on signatures, instead adopting other forms of detection. Many products have incorporated behavioral heuristics, for example, to uncover malicious activities, or they incorporate application controls that limit what applications can run.

Additionally, to reduce the growth in signature files, many vendors are using Web-based threat intelligence (to include file and URL reputation services) that can identify threatening and malicious content available on the Internet and blocking access to that content before it ever reaches the datacenter. Server security isn't just about protecting the operating system; it also must be able to understand the vulnerabilities of hosted applications in order to prevent cybercriminals from exploiting vulnerabilities and remotely compromising Web applications.

Server security has evolved to adjust to the virtualization of the datacenter (including cloud-resident servers). As enterprise IT becomes more virtual, security providers have begun to offer specialized protection to seamlessly support organizational needs for securing internal, external, and hybrid application workloads. To be effective in this setting, security solutions have to understand the hosting environment so that performance can be maximized without the loss of security functionality. And with the virtual data center, the ability to detect lateral movement and protect against attacks ("east-west traffic" challenge) is a critical new requirement.

Security must also be able leverage the native characteristics of a virtual environment to be both efficient and effective. Where it makes most sense, like server intensive activities like antimalware scanning, deploying at the hypervisor enables holistic monitoring of all virtual machines (VMs) with minimal performance impact. Where hypervisor-level security is not practical--such as in the cloud--deep integration with the environment (e.g. Amazon Web

Services [AWS], Microsoft Azure) is a requirement to enable automated discovery, security deployment, and management.

A final key requirement of best-in-class server security is that, with servers existing in physical, virtual, and cloud environments, solutions must provide a common management and policy framework that cuts across all deployment scenarios, including hybrid architectures.

Considering Trend Micro

The Trend Micro Hybrid Cloud Security Solution is a single, comprehensive offering that spans physical, virtual, and cloud deployments. Its deep integration with leading environments such as VMware vCloud Air, Amazon Elastic Compute Cloud (Amazon EC2), and Microsoft Azure makes deployment and management of security much faster and easier than traditional options, which is critically important as datacenters transition from physical to virtual and cloud environments.

At the heart of the solution, Trend Micro Deep Security is a technology product that is designed to deliver a wide range of security controls efficiently through hypervisor or agent-based approaches, optimized for each environment. Deep Security ensures that servers — whether physical servers, VMs, or cloud instances — are protected the moment they are provisioned, and it also recommends and applies only the policies that are relevant, following VMs as they are brought up and down.

As a comprehensive security offering, Trend Micro Deep Security includes the following set of controls:

- Antimalware with Web reputation to protect against constant malware attacks
- Network security, including intrusion protection (IPS) to shield unpatched vulnerabilities, and a stateful host firewall that provides a customizable perimeter around each server
- System security, including file and system integrity monitoring for compliance, and log inspection to identify and centrally report important security events
- Automated server scanning for dynamic policy application based on context

The Trend Micro Smart Protection Network, a global security network delivering timely threat data and protection rules derived from over 150 million endpoints and supported by a large team of global threat experts, underpins Deep Security.

Within a VMware environment, Deep Security can be deployed at the hypervisor level for performance-intensive operations like antimalware, delivering maximum efficiency and a holistic view of all VMs on a hypervisor, including virtual servers and/or virtual desktops (VDI). Deep Security's native integration with VMware enables it to deliver a range of security capabilities without the complexity and overhead of traditional endpoint security providers. This approach helps datacenter operators and architects control operating costs while improving performance with security optimized for virtual environments. Automatic policy management, deployment orchestration, and central management of multiple security controls help decrease risk and costs as well as save time.

The solution also offers unique value in the virtual datacenter and cloud, in that it can detect lateral movement as a part of an attack and protect against that, effectively solving the "East-West" traffic challenge. At the same time, Deep Security has the ability to very accurately detect indicators of compromise (IOCs) within a server deployment, enabling the organization to take action on any deployment that may have been compromised.

For cloud deployments, tight integration with cloud service providers, including Amazon EC2, Microsoft Azure, VMware vCloud Air, makes security efficient and elastic so that datacenters get the full benefit of the cloud's agility and cost savings. Deep Security is compatible with leading cloud deployment tools such as Chef, Puppet, and Salt, enabling agent-based security to be automatically deployed and managed consistently with the way the cloud is managed.

Trend Micro offers its security platform as software and as a service, enabling customers to align their purchasing with their datacenter strategy. Deep Security is also available on the AWS and Azure Marketplaces, providing customers with additional purchasing flexibility. Unique in the industry, and representative of Trend Micro's commitment to the cloud market, Deep Security can also be purchased on an hourly basis, aligning security to the way that the cloud is procured.

Challenges and Opportunities

Server security has been growing, and Trend Micro has been advancing the technology to address the changing nature of the datacenter. However, challenges continue to inhibit some server security deployments. The primary drag is that many organizations are not concentrating on server security. Surveys have shown that the majority of security professionals do not put server security high on their priority list. Other concerns have a greater level of interest. In security, as with many other things, the squeaky wheel gets the grease. However, with the many high-profile vulnerabilities (e.g., Shellshock, Heartbleed) and breaches that occurred in the past 18 months, it's clear that server security is one squeaky wheel that needs to be greased.

Interestingly, there has been considerable emphasis on endpoint security, but much of it is associated with mobile devices. IDC suggests that organizations concerned about endpoints should also be concerned about servers because they too are an endpoint. Indeed, servers are endpoints that have access to much more data than a mobile device typically does, and they can generally access business logic unavailable to other types of endpoints.

IDC believes that confidence in server security may be shifting as a result of virtualization and cloud security. With cloud deployments, the security staff needs greater assurance that the virtual servers have the proper protection and that on-premises personnel have visibility into the security. This should increase the emphasis on, and demand for, server security and solutions such as Trend Micro's that can provide wide-ranging security features across multiple deployment options.

Conclusion

For years, server security has been a technology asset that organizations only occasionally felt they needed; however, the changing dynamics in datacenters has elevated server security into a key component of an enterprise's IT security posture. Issues around the fluid nature of a datacenter's virtual environment, the speed of server and application

performance and deployment, and the expanding usage of cloud computing, virtualization, and social media have changed the server security landscape.

Server security prevents the injection of malware or malicious code into servers and protects the servers from attacks that may inhibit their ability to operate effectively. It includes many security functions such as antimalware, endpoint firewall, host intrusion prevention, application control, file integrity monitoring, log inspection, Web threat protection, and vulnerability containment. On top of these functions is a requirement for central management, which allows for single-pane-of-glass control across all deployment scenarios.

IDC expects server security to continue growing as a way to protect server-hosted applications. Network security, the primary security component in the datacenter, cannot be counted upon to protect server-based applications. When server applications receive requests from browsers and other clients, network security will check to see if the request contains a known network exploit or falls outside a policy setting. But network security software is unable to recognize a threat if a conforming request doesn't set off an alert unique to the application, and perimeter network security isn't relevant in the context of public cloud. Server security is the only security component able to provide that protection.

Based on these factors, IDC is forecasting server security to be a billion-dollar market by 2019. Trend Micro has been the market leader in this segment for six years in a row. The company continues to make significant investment in this space and has been adding to its solution to address new threats, new virtualization options, and support for additional cloud infrastructure-as-a-service (IaaS) providers. Trend Micro's strong security pedigree, cloud-based threat intelligence network, and server security management platform should allow the company to remain a premier provider.
