Sponsored by

Bitdefender

Newest Data Center Dilemma: Security vs. Performance

In This Paper

- Traditional IT security solutions rely on agents, which are not designed to operate in today's complex virtual environments
- The agent-based approach to security diminishes the business value of virtualization and complicates management
- Virtualized data centers require a centralized approach that eliminates the need for agents on every VM

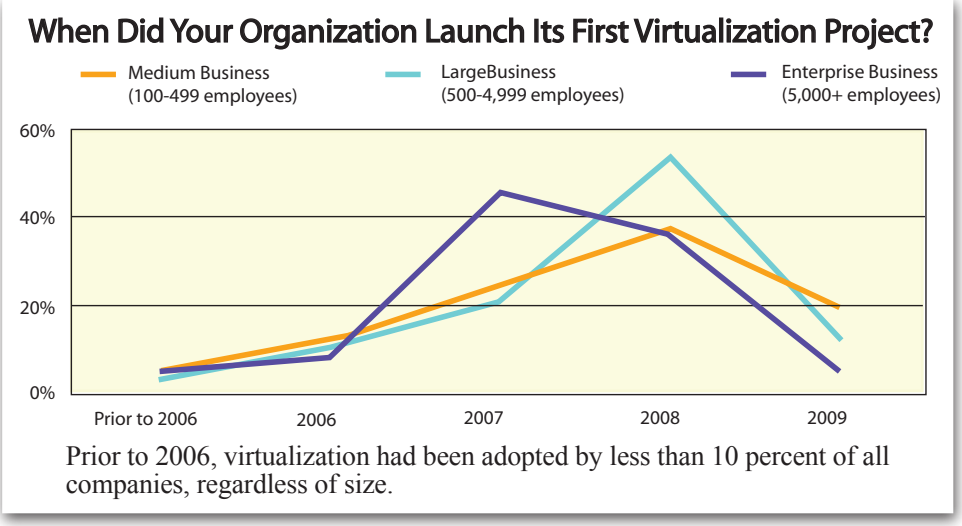
CIO INSIGHT

Executive Brief

Introduction

Virtualization has become so widespread that it's easy to forget how new this technology really is. As the graph[i] on the right shows, less than a decade ago fewer than 10 percent of companies had adopted this now-ubiquitous approach to computing. The relative "youth" of virtualization has important implications for other companion technologies — particularly security. To put it bluntly, the security systems originally designed to protect client/server architectures haven't caught up to the reality of the virtualized data center.

This Executive Brief will cover the problems traditional security solutions create for virtualized data centers, and also discuss how a centralized approach to security can address these problems.



Prior to 2006, virtualization had been adopted by less than 10 percent of all companies, regardless of size.

Security vs. Performance for the Virtualized Server

When examining the limitations of traditional client/server security solutions in a virtualized environment, it is important to bear in mind the reasons why companies have opted for virtualization in the first place. Gartner quantified these reasons in its 2012 Magic Quadrant for x85 server virtualization. According to Gartner, 60 percent of companies that adopted virtualization cited improved resource utilization as a primary reason. Reduced operational expense was close behind at 58 percent, and another cost-related item — reduced/deferred hardware capital expenses — was cited by 43 percent of respondents.

To state the obvious, these benefits all depend on the ability to host multiple virtual machines (VMs) on a single physical server — and the higher the consolidation ratio, the greater the savings. This is where traditional security solutions fall short. These solutions rely on agents, which are deployed on a one-agent-per-VM basis. Every VM must therefore maintain its own separate set of inspection engines and signature and heuristic databases. Unfortunately, the routine operation and maintenance of these agents can create conditions that substantially impact performance.

Such events, often referred to as "AV storms," occur when multiple VMs on the same physical host attempt to conduct a security-related task at the same time, and in doing so exhaust that host's resources. These tasks include:

- Simultaneous scheduled scans
- Updates involving the downloading of the latest signature and heuristic engines
- Upgrades when the antivirus engines are modified or reinstalled

"The relative "youth" of virtualization has important implications for other companion technologies — particularly security."

"Migrating to a public cloud by no means eliminates the cost problems associated with agent-based security solutions."

In data centers where many of the VMs are based on the same template, traditional security solutions impose an additional drag on performance because they end up inspecting the same identical objects (files, registry items, etc.) again and again.

The net effect of traditional security solutions is that they require companies to purchase and operate more physical servers, with all the extra power, cooling and storage that implies. In other words, traditional security solutions are in direct conflict to the fundamental resource- and cost-saving goals of virtualization.

This effect is magnified with virtual desktop infrastructures (VDIs). Because each end user VM in a VDI deployment requires far less in terms of host resources, many more VDI instances can be hosted on a single physical server. This in turn means there will be many more security agents to drain that server's resources. In one test conducted by Bitdefender, security agents increased the demand on CPU resources by 36 percent, and increased memory requirements by 11 percent[ii]. Because of these problems and others discussed below, some organizations have found themselves in the position of either accepting the creation of some VDI instances without endpoint security, or abandoning VDI altogether.

Migrating to a public cloud by no means eliminates the cost problems associated with agent-based security solutions. It is true that with a public cloud deployment, IT departments don't need to worry about how many VMs are running on any particular server. Consolidation ratios are the cloud vendor's problem. But there is another cost-related problem. Traditional security systems are normally licensed on a per-user or per-VM basis. This means organizations must estimate the number of licenses that will be required during periods of peak demand and pay for that number, even though those licenses may only be required one or two days per month. This licensing model makes no sense for companies that have migrated applications to a public cloud specifically to increase flexibility and pay only for the compute cycles, bandwidth, and memory that they actually use.

New Vulnerabilities, Complex Management

Beyond the previously discussed performance problems that directly (and negatively) impact cost, there are three other areas where traditional agent-based systems designed to protect endpoints that are physical "islands" create problems.

• **Vulnerability.** In a data center with thousands of VMs, the agent-based security solutions on some VMs are bound to become outdated when those VMs are in a dormant/offline state. At reboot, the security solution on a dormant VM must download its latest antivirus and engine signatures. This download creates a window of opportunity for a malicious exploit that lasts somewhere between five and 12 seconds. Since enterprises now sustain a malware attack every 1.5 seconds[iii], this download window is a serious problem.

• **Management.** Traditional management tools are designed to monitor and control their antivirus clients in highly static environments. In these environments, part of the server installation process is the registration of that server's security agent with the security management console. Typically, servers in such an environment remain up and running (at least most of the time) for several years. When a server is decommissioned, the entry corresponding to that server's agent needs to be manually removed from the console. In a virtualized

environment, where dozens of VMs are being instantiated and/or terminated every day, these consoles can be quickly overwhelmed with orphan entries.

• **Flexibility.** Data centers haven't been single-vendor operations for decades, and the advent of virtualization has not changed this fact. It's true that on the server side, VMware's ESXi hypervisor is dominant, but many VMs run on Citrix's Xen and Microsoft's Hyper-V. When it comes to VDI endpoints, the options for end-users seem to be multiplying almost on a monthly basis, with multiple classes of hardware (desktop, laptop, tablet, smart phone) and multiple vendors as well. On top of this, every cloud has its own quirks that must be taken into account so that applications of any kind (including security) work properly. Again, traditional security solutions were never designed for this level of diversity and complexity.

To summarize, traditional security solutions significantly diminish the business value of virtualization because of the cost burden they impose. In addition, they complicate management, and can even create new windows of vulnerability. Eliminating these problems is possible, but it requires a new approach to security, one that's specifically designed for the needs of virtualized data centers today and in the future.

Centralizing Security

The key to cost-effective security in a virtualized data center is a centralized approach that eliminates the need for resource-consuming agents on every VM. While no security solution can have a zero footprint in the VMs it protects, that footprint can be dramatically reduced by offloading the majority of the anti-malware functionality to a dedicated virtual appliance. In a centralized approach, that appliance performs scans and other related functions so there is no significant resource burden on the VMs being protected. Furthermore, since the inspection engine and signature and heuristic databases all reside on the appliance, the downloading of updates, new databases etc. has no effect on VM performance.

The key features of a centralized approach include the following:

• **Near-zero VM footprint.** This feature is by far the most important factor for boosting performance and reducing total cost.

• **Multiple endpoint capabilities.** The solution should be able to handle all types of endpoints, including traditional endpoints, VMs and BYOD mobile devices.

• **Support for a wide variety of environments.** The solution should be hypervisor agnostic for compatibility with all major hypervisors, including ESXi, Xen, Hyper-V, KVM and others, as well as OS agnostic.

• **Automation.** Manual operations associated with the provisioning and destruction of VMs should be held to a minimum.

• **Ease of management.** The solution should integrate management and reporting on one console.

• **Virtualization-oriented licensing.** The licensing model should match the needs of a virtualized environment where large numbers of VMs are provisioned and destroyed on a regular basis.

Bitdefender is a leader in advanced enterprise security solutions designed from the ground up for virtualized environments. Unlike traditional endpoint solutions, Bitdefender technologies impose no significant performance or price penalty for virtualized data centers, while providing superior security. For more information, please visit http://enterprise.bitdefender.com/.

[i] http://www.cdwnewsroom.com/cdw-server-virtualization-life-cycle-report-medium-and-large-businesses/

[ii] http://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_WP_SVE_Performance_en.pdf

[iii] http://www.infosecurity-magazine.com/news/enterprise-cyber-attacks-more-than-double-in-2013/