Endpoint Security and Virtualization

Darren Niller – Product Management Director
May 2012
Table of Contents

Introduction ...........................................................................................................................................3
Traditional Security Approach: Counteracts Virtual Performance Gains ..........................................3
Agent-less Approach: Open to Exposure ..............................................................................................4
Webroot SecureAnywhere Approach: Fast, Lightweight, Effective ..................................................5
  Webroot SecureAnywhere Performance ..............................................................................................5
  Webroot SecureAnywhere Management .............................................................................................5
Summary ..............................................................................................................................................6
  About Webroot ....................................................................................................................................6
Introduction

Besides form factor, virtual systems are not really that different than physical systems. They both use the same operating systems and applications. They both present users with computing resources such as RAM and hard drives. Consequently, the ability to exploit vulnerabilities in a physical environment will present a significant threat to virtualized environments as well.

With over 60%\(^1\) of small-to-midsized business (1-1,000 employees) and even more enterprises adopting virtualization, IT administrators need to consider how to best protect a mix of physical and virtual systems without adding complexity or reducing performance.

This paper examines the different endpoint security methods for virtualized environments and presents how Webroot Secure Anywhere Business - Endpoint Protection security provides optimal performance, protection and manageability.

Traditional Security Approach: Counteracts Virtual Performance Gains

Until recently hardware systems were designed to run one operating system, and normally only one application per server. This approach left many hardware resources (CPU, RAM, storage, network interface) vastly underutilized. With the introduction of x86 virtualization technology in the late 90’s, IT administrators started to eliminate the “one server, one application” model by creating many virtual machines (VMs) residing on a physical server (host). This provided the ability for a single physical server to handle several different application workloads while ensuring optimal performance and efficiency. Since then, a majority of IT organizations have deployed virtualization and have realized 50%-70% cost savings on their overall IT costs\(^2\).

A common method of protecting virtual systems is to deploy traditional, signature-based endpoint security, but this has created many challenges. Endpoint security was originally designed to operate in a one-to-one ratio, one endpoint client to one physical system (server or desktop). Clients on individual systems execute malware detection scans and need to be updated with the latest signature definition files at least daily. It can be viewed that the traditional-based client design have relied heavily on a one-to-one architecture, taking full advantage of storage and computing resources available on the physical system. However, definition files have become unmanageably bigger, consuming valuable storage and making updates painful. Scans are taking longer, sometimes hours. Furthermore, scans demand more and more CPU, significantly impacting system performance and productivity.

When virtualization is deployed, and traditional endpoint security is used for protection, a client is required to be located on each individual VM. The requirement of a signature based client residing on each VM will slow down performance, especially if scanning and updates take place on multiple guests simultaneously. For example, if 50 virtual machines were running on the same host, it will have 50 endpoint clients running at the same time. This is what causes the degradation of the system, affecting the performance of each VM and application, creating a phenomenon labeled an anti-virus (AV) storm. Additionally, administrators often want to rapidly deploy VMs, but the size of an AV client installation may inhibit the quick rollout of new VM. With definition files and cumbersome
product installations requiring hundreds of megabytes on each endpoint, they quickly grow to use tens or hundreds of gigabytes, even with only a small number of individual endpoints on a single VM.

**Agent-less Approach: Open to Exposure**

One method of protecting virtual systems without the negative effects of signature based clients is to use a security solution which resides within the virtual infrastructure itself.

Virtual infrastructure (VI) is the management layer that controls the interaction between each VM and the host hardware. For example, VMware has introduced vShield, an infrastructure tool that provides a specialized security solution and visibility into the file system and network traffic between each VM without the use of a client. Deploying specialized security within the VI allows each VM to be protected in an “agent-less” fashion.

While there are some obvious performance benefits realized with agent-less security, there are some security challenges that IT administrators need to consider before investing in a dedicated, virtual security solution.

First and foremost, security used only at the VI level potentially exposes a system to sophisticated threats. Agent-less security methods do not take into account threats which live in memory or do not otherwise exist as files on disk. There are several classes of threats which have begun to become more prevalent in recent years that follow these approaches, rendering themselves invisible to VI level monitoring. For example, an information stealing Trojan like Zeus exists solely within the browser's memory. When infected with a threat like this, no specialized virtual security product could detect a file as being malicious because there aren't any malicious files on the system. This tactic is currently used by dozens of the top information stealing Trojans and poses a massive risk.

Plus, VI tools do not provide visibility at the behavior level; their only ability to detect threats is by signature and it is not possible to perform generic protection on the system. For example, if a newly released malicious keylogger is running on the system and not blocked by signatures, agent-less security utilizing VI tools will be blind to the threat.

Secondly, using dedicated security utilizing virtual infrastructure tools is not ideal for cloud or physical systems. Physical systems have a single operating system, negating the need for an agent-less approach and in multi-tenant public cloud environments; administrators do not have access to VI tools. For physical and cloud based servers, protecting individual systems is the best approach. Having point security solutions to protect an environment that has different server/desktop form factors across physical, virtual and cloud presents unnecessary administrative overhead by adding more time and money to protect an entire environment.

Although there are benefits for deploying security within a virtual infrastructure, the real reason why most security vendors have developed agent-less solutions for virtual environments, is due to anti-virus (AV) storms and the fact that their standard endpoint solutions are very memory hungry. Agent-less solutions therefore leave VMs vulnerable to sophisticated attacks and add another conventional point solution just for virtual environments, which presents an unnecessary administrative burden.
Webroot SecureAnywhere Approach: Fast, Lightweight, Effective

Deploying virtual systems to achieve significant efficiency, performance and cost savings is a step most IT administrators have taken or are considering in the future. Sacrificing performance by using traditional signature-based endpoint security, or exposing your virtual environment to vulnerabilities through an agent-less approach, is not ideal.

Webroot SecureAnywhere Business - Endpoint Protection (WSAB) introduces an innovative approach to securing VMs that provides the most effective protection and far superior performance within virtual environments.

Webroot SecureAnywhere Performance

To ensure complete protection, VMs must be protected individually without impeding performance. With WSAB, each VM is protected by an extremely lightweight client (<700KB) that installs in under 63 seconds. This allows administrators to deploy new virtual machines quickly and with a faster “time to protect”, reducing overall exposure.

Many firms building virtual environments are encountering “virtual saturation”. When multiple VMs run applications concurrently and cause network resource depletion, they tax the virtual translation layer creating a bottleneck. As WSAB uses only around 12MB3 of memory during scans that last less than a minute, IT Administrators do not need to worry about AV impacting back-end and system utilization.

Additionally, WSAB intelligently tunes its memory usage when resource intensive applications are detected. The ability to run concurrent scans allows WSAB to effortlessly scale to thousands of VMs on a single physical server without a disruption or create an AV storm. It does this by scanning beneath the operating system by parsing the harddisk and registry raw. WSAB’s approach of installing within individual VMs without impacting performance cannot be replicated by other security vendors simply because of the client footprint and demand of compute resources.3

- 92% less memory than Trend Micro3
- 99 times faster install than Symantec3
- 3X faster scans than McAfee and up to 30 times faster than Symantec3

Webroot SecureAnywhere Management

WSAB leverages the cloud for management, eliminating the need to maintain local security hardware infrastructure. From a single, feature rich web console and universal client; IT administrators can manage and view their entire environment- physical desktop and servers, virtual machines and cloud-based systems. The client self-registers and does not need to be manually updated or patched, negating the need to schedule or monitor updates. IT environments with cloud-based systems do not need to worry about additional CPU or network charges due to heavy, signature-based clients. The cloud also enables Webroot to deliver a support experience unrivalled by the industry. Webroot support engineers instantly identify issues at a client level and can gather all necessary logs to diagnose and remedy a problem at the click of a button. This new approach ensures your virtual environments will run at peak performance, untethered by your endpoint security software.
Overall, the WSAB management approach provides the ability to have the best virtual protection without a dedicated or specialized security solution.

**Summary**

IT administrators managing virtual environments and other types of deployments (physical server, desktop and cloud) need a solution which maximizes the benefits gained with virtualization while maintaining absolute system protection across all systems. Webroot SecureAnywhere Endpoint Protection provides an unparalleled security approach for physical, virtual and cloud-based systems, securing an entire environment by unmatched protection and superior performance.

Officially supported to run on VMware platform:
http://vmware-alliances.force.com/supportedapps/Application?id=087500000006CExAAM

Webroot Statement of Commitment to the VM Platform:
https://na3.salesforce.com/sfc/p/5000000007rinpHbljnDYqse8gA8ovRaKgz6j0EM=

**Supported Virtual Server/Desktop Platforms:**

- **VMware:**
  - vSphere 4
  - ESX/ESXi3.0, 3.5, 4.0, 4.1
  - Workstation 6.5, 7.0, 8.0 Server 1.0, 2.0

- **Citrix:**
  - XenDesktop 5
  - XenServer 5.0, 5.5, 5.6

- **Microsoft:**
  - Hyper-V Server 2008, 2008 R2.6

**About Webroot**

Webroot is committed to taking the misery out of Internet security for businesses and consumers. Founded in 1997, privately held Webroot is headquartered in Colorado and employs approximately 400 people globally in operations across North America, Europe and the Asia Pacific region.

Webroot Headquarters: 385 Interlocken Crescent, Suite 800, Broomfield, Colorado 80021 USA

**References:**

1. Spiceworks, State of SMB IT, 1H 2012
4. http://www.av-test.org/en/tests/test-reports/test-reports/?tx_avtestreports_pi1%5Breport_no%5D=120525