Endpoint Security and Virtualization
INTRODUCTION

Aside from form factor, virtual systems are not very different from physical systems. They use the same operating systems and applications and provide users computing resources such as RAM and hard drives. Consequently, the ability to exploit vulnerabilities in a physical environment presents a significant threat to virtualized environments as well. In addition, virtual environments are also targets for unique threats.

With over 60%¹ of small to medium-sized businesses (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 90s, 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 costs².

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. The traditional client design relies heavily on one-to-one architecture, taking full advantage of storage and computing resources available on the physical system. However, definition files have become increasingly unmanageable, 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 must be installed 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, 50 endpoint clients will be running at the same time. This is what causes the degradation of the system, affecting the performance of each VM and application, creating labled an antivirus storm. Additionally, administrators often want to rapidly deploy VMs, but the size of an antivirus 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.

AGENTLESS 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 “agentless” fashion.

While there are some obvious performance benefits realized with agentless 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. Agentless 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 are becoming 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.

Additionally, 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, agentless
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 agentless 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. Using dedicated security solutions to protect an environment for just virtual machines presents an unnecessary administrative overhead.

Although there are benefits for deploying security within a virtual infrastructure, the real reason why most security vendors have developed agentless solutions for virtual environments, is due to anti-virus storms and the fact that their standard endpoint solutions are very memory hungry. Agentless solutions therefore leave VMs vulnerable to sophisticated attacks and add another conventional solution just for virtual environments, which presents an unnecessary administrative burden.

**THE WEBROOT® 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 agentless approach, is not ideal.

Webroot SecureAnywhere® Business – Endpoint Protection 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 Webroot SecureAnywhere Business – Endpoint Protection, each VM is protected by an extremely lightweight client (<700KB) that installs in under 6.3 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 Webroot SecureAnywhere Business – Endpoint Protection uses only around 12MB of memory during scans that last less than a minute, IT administrators do not need to worry about an antivirus solution impacting back-end and system utilization.

Additionally, Webroot SecureAnywhere Business — Endpoint Protection intelligently tunes its memory usage when resource intensive applications are detected. The ability to run concurrent scans allows Webroot SecureAnywhere Business — Endpoint Protection to effortlessly scale to thousands of VMs on a single physical server without disruption or creating an antivirus storm. It does this by scanning beneath the operating system, parsing the hard disk and registry raw. The Webroot approach of installing within individual VMs without impacting performance cannot be replicated by other security vendors simply because of the client footprint and demand for computing resources.

- 99.6% less memory than Trend Micro
- 97% faster install than Symantec
- 6x faster scans than McAfee and up to 11 times faster than Symantec

**Webroot SecureAnywhere® Management**

Webroot SecureAnywhere Business — Endpoint Protection 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 virtual environments run at peak performance, untethered by your endpoint security software.

Overall, Webroot management approach provides the ability to have the best virtual protection without a dedicated or specialized security solution.

**SUMMARY**

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 Business — Endpoint Protection provides an unparalleled security approach for physical, virtual and cloud-based systems, securing an entire environment with unmatched protection and superior performance.
Officially supported to run on VMware platform:
http://vmware-alliances.force.com/supportedapps/Application?id=0875000006CExAAM
Webroot

Statement of Commitment to the VM Platform:
https://na3.salesforce.com/sfc/p/500000007rinpHbljnDYqse8gA8ovRaKgz6j0EM=

Supported Virtual Server/Desktop Platforms:

VMware:
» vSphere 4
» ESX/ESXi 3.0, 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

References
1 Spiceworks, State of SMB IT, 1H 2012
2 http://www.vmware.com/virtualization/virtual-machine.html
4 http://www.av-test.org/en/tests/test-reports/test-reports/?tx_avtestreports_pi1%5Breport_no%5D=120525

About Webroot
Webroot is bringing the power of software-as-a-service (SaaS) to Internet security with its suite of Webroot SecureAnywhere® offerings for consumers and businesses, as well as offering its security intelligence solutions to cybersecurity organizations, such as Palo Alto Networks, F5 Networks, Corero, Juniper, and others. Founded in 1997 and headquartered in Colorado, Webroot is the largest privately held Internet security organization based in the United States – operating globally across North America, Europe and the Asia Pacific region. For more information on our products, services and security visit: www.webroot.com, the Webroot Threat Blog: http://blog.webroot.com or Webroot on Twitter: http://twitter.com/webroot.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George’s Quay Plaza
George’s Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900

© 2014 Webroot Inc. All rights reserved. Webroot, SecureAnywhere, Webroot SecureAnywhere, Webroot Intelligence Network, and WIN are trademarks or registered trademarks of Webroot Inc. in the United States and/or other countries. Microsoft, Windows, Windows Vista, and Internet Explorer are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Mozilla and Firefox are registered trademarks of the Mozilla Foundation. All other trademarks are properties of their respective owners.