
Bitdefender® ENTERPRISE
WHITE PAPER
Securing the virtual infrastructure without impacting performance
Bitdefender

Introduction

Virtualization offers many benefits, but also raises additional performance issues in areas of security. This bodes the question: is virtualization security counterproductive? Moreover, do the currently-available security solutions impact some of the benefits offered by virtualization, creating bottlenecks and additional issues in virtualized environments as compared to physical server environments?

This paper aims to explore some of the challenges specific to virtualization security, provide results of several performance tests conducted by Bitdefender, and offer insight into the Bitdefender hypervisor agnostic Security for Virtualized Environments (SVE) solution.

Virtualization security pitfalls

Agent-based antimalware solutions installed on virtual machines will at one time or another become outdated due to the dormancy of a virtual machine in an offline state. This is a known fact. When the virtual machine is restarted, the security solution must download its latest antivirus and engine signatures, as well as the latest software updates. This update process alone can take anywhere between 5 to 12 seconds, which creates a window of opportunity for malicious intent.

An alternative to legacy antimalware solutions is to take advantage of security solutions that have integrated with VMware Endpoint Security to provide an agentless solution. The agentless approach most certainly does mitigate boot latency and outdated anti-virus protection issues. However, there are some pitfalls to this approach:

- VMware is currently the only vendor to offer the agentless capability through integration with vShield Endpoint. For organizations using vendors with Xen or Hyper-V hypervisors, there simply is no agentless solution available. Moreover the agentless solution is limited to Windows environments only. Linux based and non-VMware environments still need to use traditional agent-based solutions.
- Although the term agentless has been coined, it not entirely true. In fact one needs to install the vShield Endpoint driver on each virtual machine to be protected.
- There are also limitations to the agentless solution, in that only file-based scanning is supported. Memory and registry scanning, behavioral monitoring and application, as well as device control still require the use of traditional agent-based solutions.

The illustration below shows Bitdefender's agentless security through the integration with VMware vShield Endpoint security. However, for organizations using other virtualization solutions, Bitdefender does have a solution that is designed to work with any virtualized infrastructures.

Consolidation ratios scenario

One of the main drivers of virtualization is the cost savings derived from virtual machine consolidation ratios – attaining the maximum number of virtual machines running on one host. Security should be designed specifically for virtualization, with minimal impact to the virtual environment, thus enabling maximum virtual machine consolidation ratios.

Sizing the hardware requirements for a virtual environment can vary quite significantly from one environment to another; it is very much dependent on the type of applications that will be running in the virtual environment. The CPU, memory, network and storage performance needs to be considered based on the type of virtual machines that will be running within the environment. For example, a higher virtual machine consolidation ratio will be achieved with web application virtual machines compared to virtual machines running database applications. Depending on the application, it is always recommended to allocate at least 20% from the system resources pool for utilization peaks.

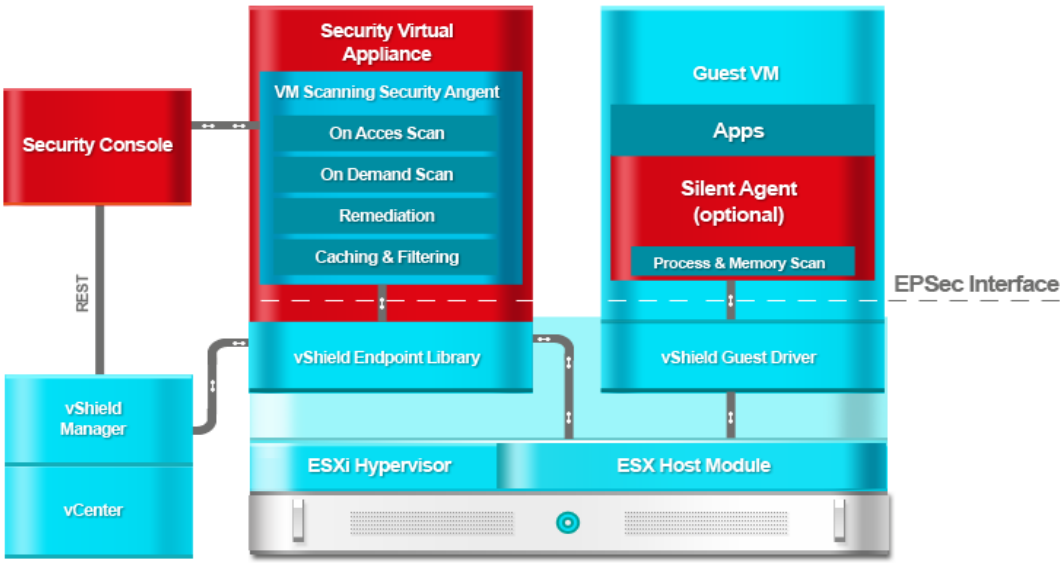
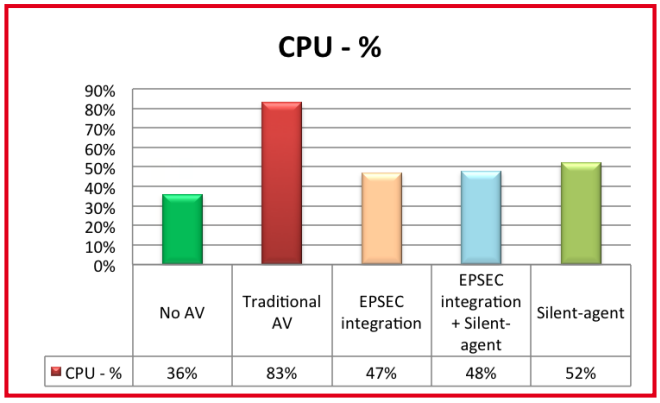
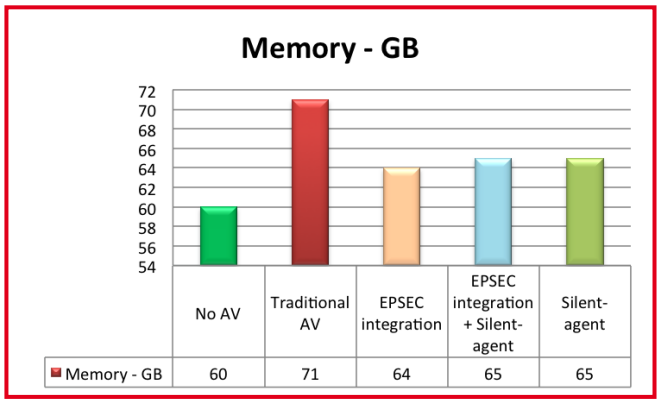


Figure 1: Security for Virtualized Environments – VMware EPSEC integration

Attention should also be paid to the impact that security will have on the environment, as shown by the following performance test results. Please refer to the appendix for test environment information.





With traditional antimalware, the consolidation ratio obtained during the tests was of 45 virtual machines per host server. Using the VMware Cost-Per-Application calculator[1], the average cost per VM based on the given configuration would be $1358.19. CPU and memory utilization is shown for the following configurations:

- SVE in an agentless configuration integrating with VMware vShield Endpoint Security (EPSEC)
- SVE in an agentless configuration integrating with VMware vShield Endpoint Security (EPSEC) + the SVE Silent Agent
- SVE Silent Agent only

The performance results tend to speak for themselves: traditional agent-based antimalware use approximately 36% more CPU (83-47) and 11% (7/64) more memory than the vShield-integrated SVE solution. The performance impact caused by traditional antimalware would result in the need to purchase additional hardware, which translates into additional potential cost per VM before even considering the licensing costs for the antimalware solution.

[1] VMware Cost-Per-Application Calculator

Based on the performance testing results, a good assumption would be that SVE enables customers to have at least 20% more virtual machines per host compared to traditional antimalware solutions, in any virtualized environment.

Optimized virtualization security

Security for Virtualized environments (SVE) by Bitdefender is designed to work with any virtualized environment, enabling customers to achieve higher consolidation ratios on each host server, when compared to traditional security solutions. This results in improved cost savings in areas like hardware, storage and cooling requirements, therefore allowing customers to increase the return on investment for their virtualization project. To ensure higher cost efficiency, Bitdefender's solution leverages patent-pending technologies and optimization mechanisms, some of which will be hereafter described in further detail.

Centralized scanning for any virtualized environment

SVE is designed as a hybrid security solution, adaptable to the mixed and dynamic datacenters today. As opposed to legacy security, Bitdefender implements centralized scanning by offloading much of the antimalware functionality on a dedicated hardened virtual appliance called the Security Virtual Appliance (SVA). This approach optimizes both on-access and on-demand scanning processes while deduplicating critical computing resources on the host servers. Process and memory scan functionality is enabled through the Silent Agent, a very small piece of software installed on the guest machines.

Silent Agent provides integration with Windows Security Center and informs the user on the protection status and event history within the VM. In VMware environments, the Silent Agent is used only for memory scanning, while on demand and on access system file scanning is handled by the vShield Endpoint driver. On other platforms and operating systems, Silent Agent enforces security policies and offloads antimalware processing to the Security Virtual Appliance through the TCP/IP protocol.

On-demand scanning of the environment is performed sequentially (VM-by-VM). With only one driver and service installed per virtual machine, there is a low system resource usage and the impact on each host server is minimal. The average footprint in vShield-integrated environments is 15 MB of disk and 20MB memory utilization.

Enhanced performance with caching mechanisms

Bitdefender's Security for Virtualized Environments employs a unique patent-pending caching mechanism whitelisting common operating system files and applications. This process significantly improves the scanning performance of virtual machines, and is updated on a continuous basis. This is achieved through two layers of cache that the solution utilizes, one of which is a self-learning cache, built into the SVA. The Silent Agent employs a local cache that is prepopulated based on its environment variables, in doing so, it is able to offload the scanning of only what is required while excluding objects that are safe.

Bitdefender

Bitdefender's Security for Virtualized Environments employs a unique patent-pending caching mechanism, whitelisting common operating system files and applications. This process significantly improves the scanning performance of virtual machines, and is updated on a continuous basis. This is achieved through two layers of cache that the solution utilizes, one of which is a self-learning cache, built into the SVA. The Silent Agent employs a local cache that is prepopulated based on its environment variables, in doing so, it is able to offload the scanning of only what is required while excluding objects that are safe.

Conclusion

Virtualization security should not hamper the performance of a virtualized datacenter environment, thus sacrificing many of the benefits of virtualization in the first place. Security for Virtualized Environments (SVE) by Bitdefender solves this problem through its unique approach to protecting virtual machines across any virtualization technology. The architecture of Security for Virtualized Environments by Bitdefender isolates the scanning functionality from systems that are being protected, removing many of the virtualization security issues outlined earlier. Additionally, Bitdefender's solution helps increase security performance by employing advanced patent-pending caching mechanisms. This results in higher consolidation ratios in virtualized datacenters, which eventually saves operational costs without sacrificing security.

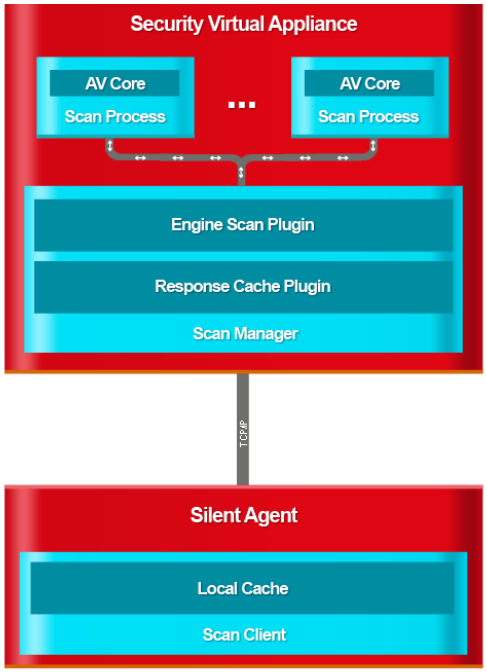


Figure 2: Scanning architecture overview

Appendix

Performance testing was conducted on the following hardware equipment and virtualization platforms:

Hardware Specifications	1x HP ProLiant BL460c G7
	2 * Xeon 6 CORE + HT @ 2.53 GHZ (Intel Xeon E5649)
	144GB RAM
	1.2 TB PCI-E SSD iSCSI storage(10 GBit)
VDI Infrastructure	20x Windows XP SP3 (32bit), 1xCPU, 1GB RAM
	20x Windows 7 (64bit), 1xCPU, 2GB RAM
	5x Windows 2k8 R2, 1xCPU, 6GB RAM
Virtualized platforms	Citrix XenServer 6.0 + XenCenter 6.0
	Citrix XenDesktop 5.5
	VMware ESXi 5.0 + vSphere 5.0

About Bitdefender

Bitdefender is a global company that delivers security technology in more than 200 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning security technology, for businesses and consumers, and is one of the top security providers in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has created the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with some of the world's leading virtualization and cloud technology providers.

Bitdefender