Bitdefender

Solution Paper

# The 8 Differences Between "Agentless" Security and BD Tools

Bitdefender

## The Problem

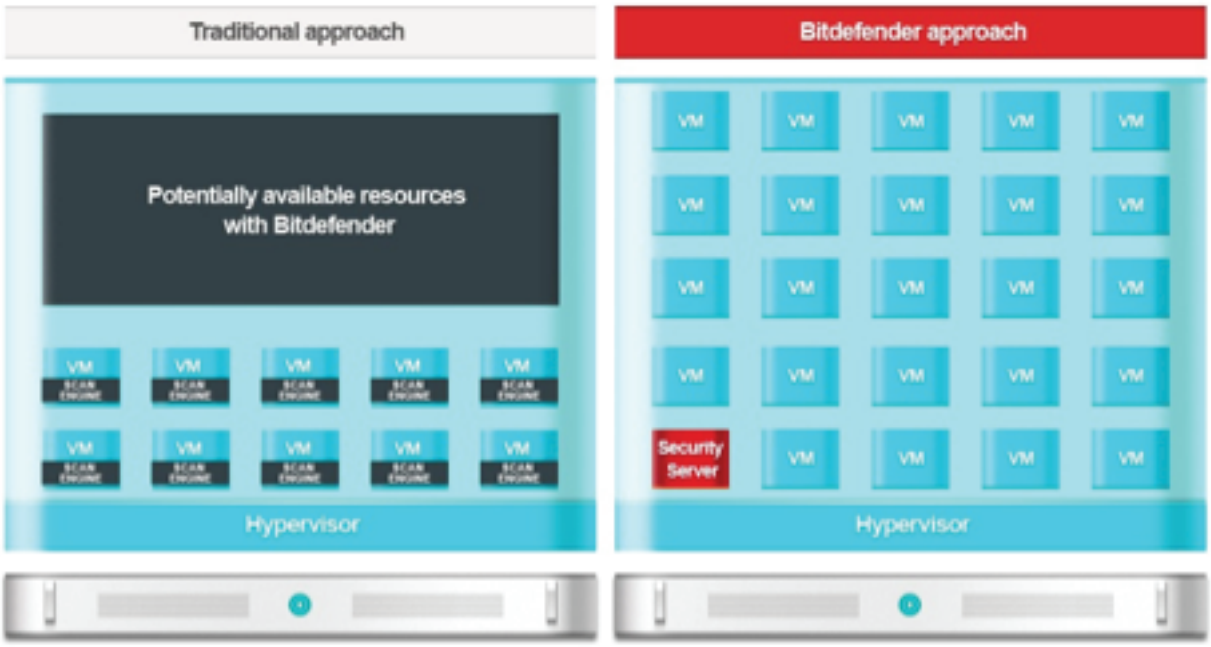
In virtualized environments, traditional antivirus solutions create performance bottlenecks due to their architecture. Traditional architectures include a full antivirus agent at each endpoint. That agent uses local data stores for signatures and other information, and must be updated frequently. The agents themselves must also be upgraded from time-to-time. This creates a duplication of footprint across environments, and duplication of maintenance.

Also duplicated are scanning results. Since they are designed to operate on isolated hardware islands, traditional antivirus agents perform scanning and analysis independently. While virtualized environments tend to have many VMs spawned form only a few templates, traditional antivirus will scan those same VMs individually, over and over again.

The worst case scenario occurs when all traditional antivirus agents are performing the same task simultaneously. That may be pushing-out an update, installing an upgrade, or performing a scheduled full-system scan. The result of the simultaneous network, CPU, memory, and storage consumption across many VMs on shared hardware is often referred to as an AV Storm. During these episodes, entire hosts may become unresponsive as hardware resources are strained, resulting in a self-induced denial of service.

## The Solution

In a nutshell, duplicating endpoint security resources within each and every virtualized endpoint is the root of the problem. The solution is to centralize and deduplicate endpoint security. That is accomplished by offloading antimalware scanning to a dedicated server.



Centralizing antimalware functionality at a dedicated system involves solving a remote scanning problem. There are a couple of different ways to solve that problem.

The first is integration with an API provided by the virtualization vendor. Today, only VMware provides this type of API; vShield Endpoint. vShield provides a file system driver embedded in VMware Tools. Marketed as "agentless", the term actually refers to the absence of security vendor software installed in the protected VMs. The security vendor integrates with vShield at the virtual appliance, providing the antimalware scanning and, when needed, taking action by calling vShield functionality.

The second method is for the security vendor to create a method of remote introspection. As with vShield, a component within protected VMs is needed to facilitate inspection and communication with the virtual appliance.

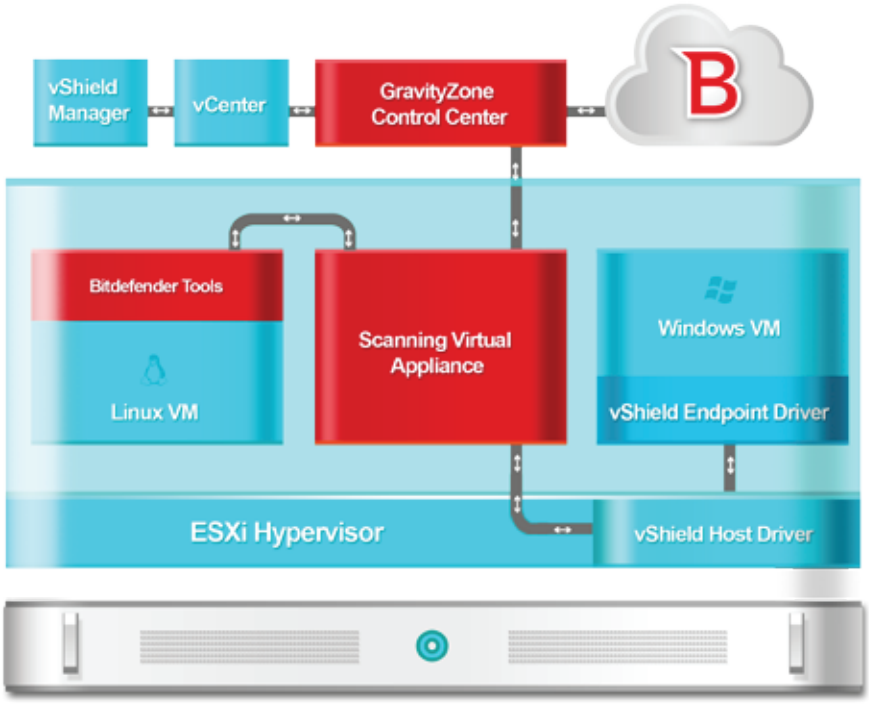
The solutions are similar in what they accomplish; offloading scanning tasks from individual VMs such that they are performed at a virtual appliance. However, when the security vendor controls the remote introspection mechanism, they have complete control of the solution. This has several implications which are detailed below.

Today, most security vendors that offer virtualization-specific antimalware exclusively use vShield Endpoint integration. The effort involved in creating a scanning offload method is innovation barrier that many vendors cannot overcome. Indeed, not every vendor has been able to develop a successful vShield Endpoint integration, instead using work-around functionality to partially address performance bottlenecks. Some of these features strain credibility, such as "randomized scheduled scans" aimed at avoiding concurrent VM scanning, while also creating a tidily self-contained oxymoron. To address performance issues when issuing updates, some vendors have also created functionality to gradually distribute the updates over time, essentially delaying time-sensitive operations as a feature.

While there are differences in offloading approaches, vendors who do have mature functionality performing offloading can be said to have virtualization-specific antimalware offerings, and should be preferred over vendors with work-around functionality. Therefore, when evaluating solutions, have vendors answer the following questions:

- Is offloading of scanning functionality from VMs to a virtual appliance performed?
- What is offloaded, and how, exactly (vShield Endpoint integration, vendor-supplied functionality)?
- Is the virtual appliance a Linux-based VM, or is it actually software that is installed on a Windows or Linux VM?
- Does the management console integrate with the virtualization management system (vCenter, XenServer, etc.)?
    - How does the management console deal with new VMs and VMs that have been deleted?
    - To which objects (groups, resource pools, and so on) can policy be applied?

- Which VM operating systems are supported, and are all features available on all operating systems (i.e., is there a difference between VDI and servers, or Windows and Linux)?
- Which hypervisors are supported?




# Agentless Versus BD Tools

## Hypervisor Support

vShield Endpoint is supported on only VMware ESXi. BD Tools is supported on a wide variety of hypervisors since the solution is independent of the underlying hypervisor. Supported hypervisors include ESXi, Xen, Hyper-V, KVM, RedHat, etc. This allows the solution to run in mixed environments and in infrastructures that do not use VMware, such as Amazon Web Services EC2.

## VM Operating System Support

vShield Endpoint supports only Windows operating systems. BD Tools supports both Windows and Linux operating systems.

## Dependencies

To use vShield Endpoint, vShield Manager (delivered as a virtual appliance) must be installed and licensed. Security for Virtualized Environments is a self-contained solution, using only Bitdefender software for security management and enforcement.

Every security vendor using vShield Endpoint is constrained by the functionality provided. To perform

additional tasks, the security vendor must install additional software. The performance of solutions that leverage vShield Endpoint is also constrained. While VMware is supportive of security vendors using vShield Endpoint, updates and new functionality are very rarely released.

In the case of Security for Virtualized Environments, Bitdefender has complete responsibility for, and control over, the antimalware solution from the management console, to the virtual appliance, and down to the BD Tools running in protected VMs. This means that when new functionality is developed, performance improvements created, or other tweaks and enhancements are needed (for example, supporting a new version of Windows), Bitdefender is the sole vendor that needs to implement changes. Further, troubleshooting is also simplified by not having multiple vendors involved in a single solution.

## Host Centricity

vShield Endpoint is provided via the ESXi hypervisor, and so the implementation is tied to each host running ESXi. The solution lacks the ability to perform tasks between hosts. This means that each host must have a virtual appliance to offload scanning to, and due to limitations of the solution, only one virtual appliance.

Security for Virtualized Environments is not tied to the hypervisor, therefore communication between hosts is supported. Hosts can have one or more virtual appliances for scanning offload, or use a virtual appliance on a different host.

This has significant implications in many environments. With vShield, the virtual appliances cannot be migrated from host-to-host. In environments where the underlying host system is unknown, including many public cloud (infrastructure-as-a-service) offerings, vShield is unusable. Since BD Tools can use a virtual appliance on any reachable host, Security for Virtualized Environments is ideal for environments where host-to-host migration is common, or the host on which protected VMs is running is not known. For example, a version of Security for Virtualized Environments is available as a service, billed hourly per-instance, in Amazon Web Services Marketplace (https://aws.amazon.com/marketplace/pp/B0096BADNI).

## Fail-over Between Virtual Appliances

The enforcement point provided by vShield Endpoint cannot communicate with a virtual appliance on a different host. Each host can have only one virtual appliance. With these two limitations, VMs protected using vShield Endpoint cannot fail-over between virtual appliances.

The BD Tools component is able to communicate with a virtual appliance on a different host, and any number of virtual appliances can coexist on each host. Fail-over between virtual appliances is a core feature of Security for Virtualized Environments.

## In-VM User Interface

Technically, vShield Endpoint does not require any security vendor software in protected VMs. File system introspection and enforcement action is handled by VMware software included in VMware Tools. However, vShield Endpoint does not include a graphical interface in protected VMs.

BD Tools does provide a graphical interface for end-users in protected VMs. If vShield is not present, BD Tools is the only component required. If vShield is present, a version of BD Tools is also installed to provide an interface, among other vital functionality.

While in a server environment, an interface in protected VMs may be considered unnecessary; in practice, it is very helpful. In cases where server administrators don't have access to security management software, an in-VM interface is the only practical way that they can understand what antimalware software is doing.

Of course, in virtual desktop environments, a local interface is a must-have. If antimalware software is taking action, such as quarantining or deleting malicious files, without an interface, the end-user will have no idea what the antimalware is doing. This will surely lead to support calls and a great deal of frustration.

## Memory and Process Scanning

vShield Endpoint is focused solely on file system activity. It does not perform any memory or process scanning. BD Tools can be layered on top of VMs protected using vShield Endpoint, or used to protect VMs without vShield Endpoint. In both cases, BD Tools provides on-demand memory and process scanning which is also offloaded from protected VMs to a virtual appliance.

## In-VM Footprint

The marketing term "agentless" implies that there is no footprint in VMs protected using vShield Endpoint. This is somewhat misleading as the phrase is used to indicate that security vendor software does not technically need to be present in protected VMs. However, antimalware offloading, which is also described as remote introspection, is not possible without a footprint in protected VMs. In the case of vShield Endpoint, the footprint is the vShield Thin Agent that is included in VMware Tools.

Though one can access files and directories remotely on a Windows system (provided that one has a valid username and password, permissions are set, and so-on), deeper access is needed to accomplish proper antimalware scanning from a remote system. A key component, then, is a file system driver to gain deep access to file system events, and a communication point to facilitate the remote aspect of remote introspection. These components are quite small, and so the disk and memory footprint of either vShield Endpoint or BD Tools is negligible.

The advantage of both approaches comes from moving much of the scanning functionality from protected VMs to a virtual appliance. This includes moving scanning engine and associated databases to the virtual appliance(s), vastly reducing the memory, disk, storage, and CPU footprint/ impact on the protected system.

While there are advantages to centralizing and deduplicating much of the antimalware functionality, not all of it should be removed from protected VMs. For example, to properly scan certain packed files, they should be unpacked on the VM, not moved to a virtual appliance and unpacked. This makes sense because antimalware engines do not scan entire files. Instead, they examine file

information (the first blocks of the file) and then request specific parts of the file based on the file information. This cannot be done if the file is packed, therefore if it is to be scanned, it must be unpacked. Unpacking on the VM and sending only specific file parts to a virtual appliance makes far more sense than transferring potentially very large files in their entirety.

Overall, while “agentless” is a catchy phrase, it is grossly misleading.

## Conclusions and Notes

In virtualized environments, centralizing and deduplicating as much antimalware functionality as is practical provides tremendous performance benefits. When consolidation ratios reach a certain level, resource bottlenecks created by traditional antivirus solutions will inevitably cause problems. To relieve resources bottlenecks, offloading antimalware functionality to a virtual appliance is a must. However, this creates a remote introspection problem that can be solved using vShield Endpoint or mechanisms created by a security vendor.

vShield Endpoint provides solid remote introspection capabilities to facilitate antimalware scanning offloading for vendors that are not able to create their own solutions. It lowers the innovation barrier for these vendors, which benefits customers by providing multiple solutions to choose from. However, as with many “easy” solutions, it has significant limitations.

Bitdefender has created Security for Virtualized Environments to provide customers with options. While the solution is integrated with vShield Endpoint, is also provides independent functionality based on BD Tools. The solution addresses limitations introduced by vShield Endpoint. The most significant advantages are hypervisor and VM operating system support, fail-over capabilities, and memory and process scanning.

What often is lost in discussions about antimalware in virtualized environments is, strangely, security. Whether or not a vendor performs offloading, if they have a poorly performing engine, they can provide only poor security, regardless of the architecture of the antimalware solution. Memory and process scanning, in addition to real-time file system protection

Due to this wide support matrix, SVE was the first security solution to gain Citrix Ready (http://blogs.citrix.com/2012/11/26/bitdefender-is-citrix-ready/) status for VDI-in-a-Box, and other Citrix solutions.

For more information about GravityZone and Security for Virtualized Environments, including a free trial, refer to:

- http://enterprise.bitdefender.com/solutions/gravityzone/
- http://enterprise.bitdefender.com/solutions/gravityzone/virtualization-security.html

1. David K Johson's post: http://blogs.forrester.com/david_johnson/13-04-01-has_vdi_peaked_a_change_in_the_adoption_drivers_sheds_new_light_and_new_life)
2. http://blogs.citrix.com/2013/07/08/top-5-scenarios-for-xendesktop-on-windows-azure/

## About Bitdefender

Bitdefender is a global company that delivers security technology in more than 100 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.





BDE-100614-SP_MS-Agentless-en_EN