White Paper

unfollow the traditional

Bitdefender®

The impact of virtualization security on your VDI environment

TESTED WITH LOGINVSI

Contents

Introduction

Virtualization provides organizations with many costs savings and significant business agility. One virtualization technology that many organizations take advantage of is called virtual desktop infrastructure (VDI). VDI empowers employees and employers with many benefits, no matter the size of the organization. One such benefit with VDI is the ability to provide centrally managed desktop environments to employees on any device. In doing so, the organization can rest assured that information is always accessed and managed in a secure fashion – regardless of where the user is accessing information from.

VDI is not for everyone. Yet it does serve a purpose in production environments like call centers that have a high concentration of task-based workers, or to replace large scale office-based desktop deployments. However, as with any environment security should always play a pivotal role and should complement the business environment. With VDI it's no different; security should be seamless, without any effect on the user experience. Designed for physical environments, traditional security can hamper VDI deployments, thus reversing the purpose of adopting virtualization or VDI in the first place – efficiency, flexibility and cost savings.

This paper provides details about performance testing conducted using industry standard tools like Login VSI. The test results show the comparison of four security solutions available on the market today that have been specifically designed for virtualized environments. These test results are aimed to help organizations gain better insight into the sizing requirement and expected performance from their VDI deployments with optimized virtualization security.

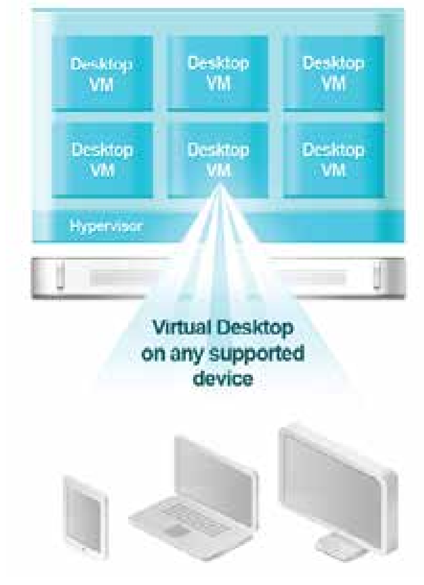


Figure 1: Virtual Desktop Infrastructure

What is VDI?

Virtual desktop infrastructure (VDI) is the practice by which a desktop operating system is hosted within a virtual machine. The virtual machine can be hosted in the organizations datacenter or from the cloud as a service (DaaS). In doing so, the VDI can be accessed from devices like thin clients, refurbished PCs, smartphones, tablets and so on. This provides organizations with the ability to guarantee quality end-user experience, regardless of the device used to connect to the corporate network.

Virtualization security challenges

It is a well-known fact that antimalware software is quite simply a requirement today. Applications and operating systems running in physical, virtual or cloud-based environments are all susceptible to exploitation. Although traditional security can be used in virtualized environments, it is neither built nor optimized for virtualized environments.

Using traditional antivirus solutions can result in specific challenges in a VDI environment such as:

- Low virtual machine consolidation ratios
- Boot latency
- AV storms
- Outdated AV on dormant virtual machines
- Management challenges

Consolidation ratios suffer as a result of using traditional security in virtual environments. Traditional security treats each virtual machine on a silo basis; it is not designed to evaluate all the virtual machine instances in a specific network or group. All application and user actions performed within the virtual machine instance are evaluated by the security agent within the operating system. This silo effect creates significant duplication, from signature databases to scan results for the same files, ultimately creating a performance problem, subsequently lowering virtual machine consolidation ratios.

Boot latency is the result of using traditional antimalware in virtual environments. When a virtual machine is started, the security solution must download its latest antivirus engine signatures, and 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.

AV storms occur when the traditional security solution agents installed on each virtual machine attempt to perform an update or a scheduled scan at the same time. In doing so, the host CPU, memory and IOP are overloaded, resulting in poor virtual machine performance and in some cases total host failure.

Outdated AV on dormant virtual machines brings the management of traditional antimalware security solutions full circle. Antimalware agents installed on dormant virtual machines can only be updated when the virtual machine is started, which results in boot latency issues and potentially AV storms, leaving the VM unprotected by the most current engine signature files.

Management of traditional security solutions can become tedious; this is especially the case in larger deployments. Each time a new traditional agent is installed, it is registered to the security management console, for administration. When a virtual machine is deleted or dormant, the traditional agent still remains registered with the security console and the only way to remove that entry is manually. This can become a laborious, mundane task, especially for large organizations where virtual machines are constantly on the move.

Choosing the right virtualization security solution

Bitdefender used Login VSI to test Bitdefender against seven virtualization security solutions available on the market today. The results capture the impact of the solutions on a VDI environment.

Login VSI is the industry standard VDI benchmarking tool that simulates typical user behavior in VDI environments.

The tool measures the total response time of several specific user operations being performed within a desktop workload in a scripted loop. There are two values in particular that are important to note: The Baseline and the VSImax.

- The VSImax is the maximum number of VDI sessions attainable on the host before experiencing degradation in host and VDI performance.
- The Baseline is the measurement of the response time of specific operations performed in the desktop workload when there is no stress on the system which is measured in milliseconds (ms).

A low Baseline indicates a better VDI user experience. When interacting with a VDI instance, if response times are too long, the ideal experience of a virtual desktop behaving like a local one is unachievable. Very long response times are akin to working with a dynamic web page that takes extended periods to refresh.

All of these measurements represent what is achievable with a given stack. In this testing, the same hardware, virtualization software, and other factors are the same across all tested solutions. The only element changed from test to test was the antimalware solution. The only way to achieve better results with the same software stack is to add more computing power, increasing costs.

Note that the Bitdefender, McAfee Multiplatform and Kaspersky Light Agent solutions do not use VMware vShield Endpoint, while all other solutions do rely on it. Bitdefender does include vShield integration for customers who wish to use it.

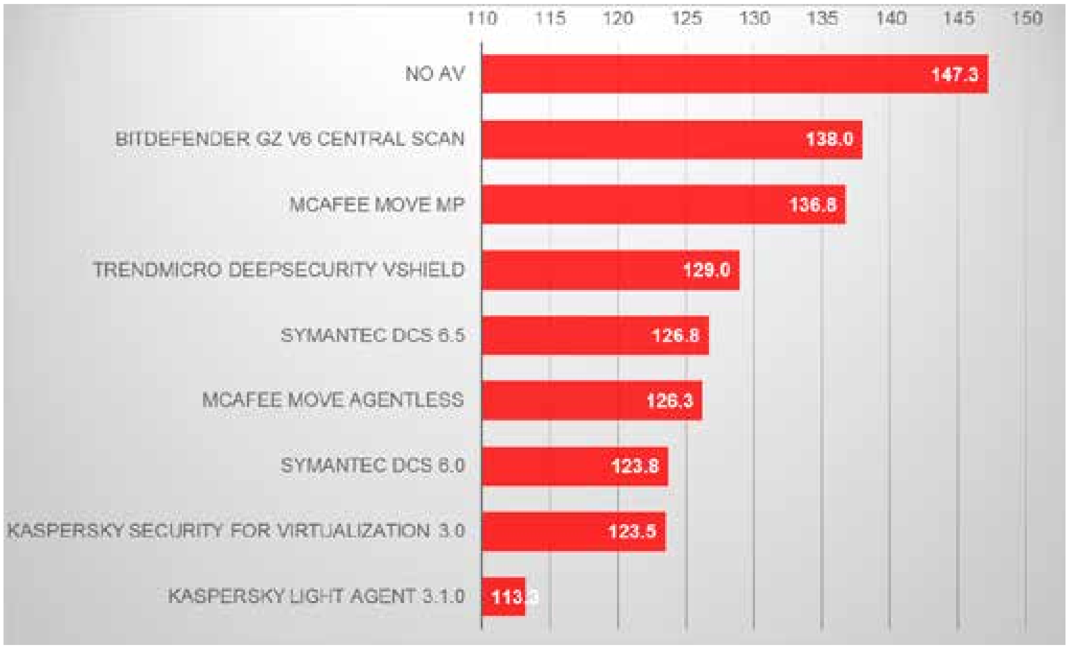


Figure 2: VSImax – the maximum attainable number of VDI sessions

The Baseline is the measurement of the response time of specific operations performed in the desktop workload when there is no stress on the system which is measured in milliseconds (ms). depicts the VSImax of each solution tested. This is the most straightforward test, representing the number of VDI instances that can be run before user experience degrades beyond unusable levels. While all tests are related to consolidation ratios, this test represents what is achievable, even with less-than-ideal user experience, in an environment.

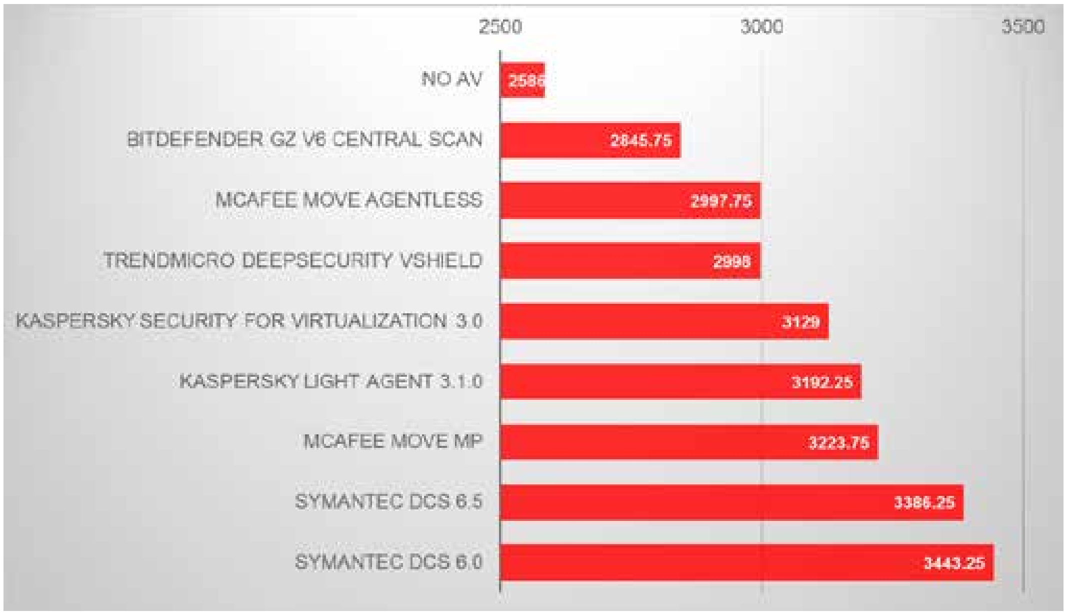


Figure 3: Baseline – the response time (ms) of an unstressed system

Figure 3 outlines test results of the Baseline measurement. Bitdefender achieves the lowest Baseline response time, which results in better user experience and desktop workload performance when the environment is not stressed.

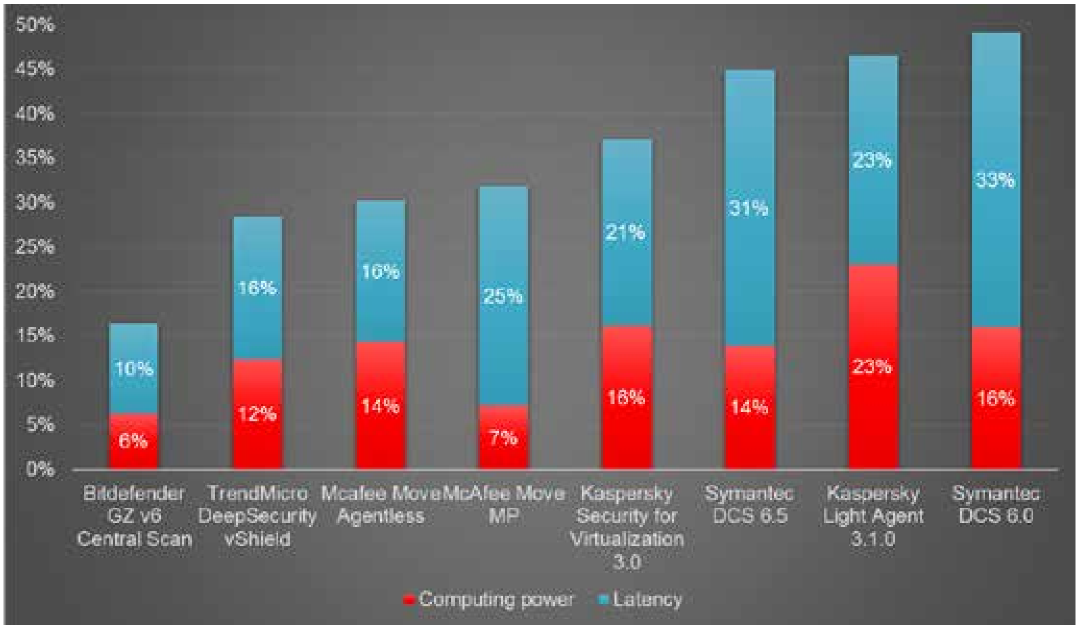
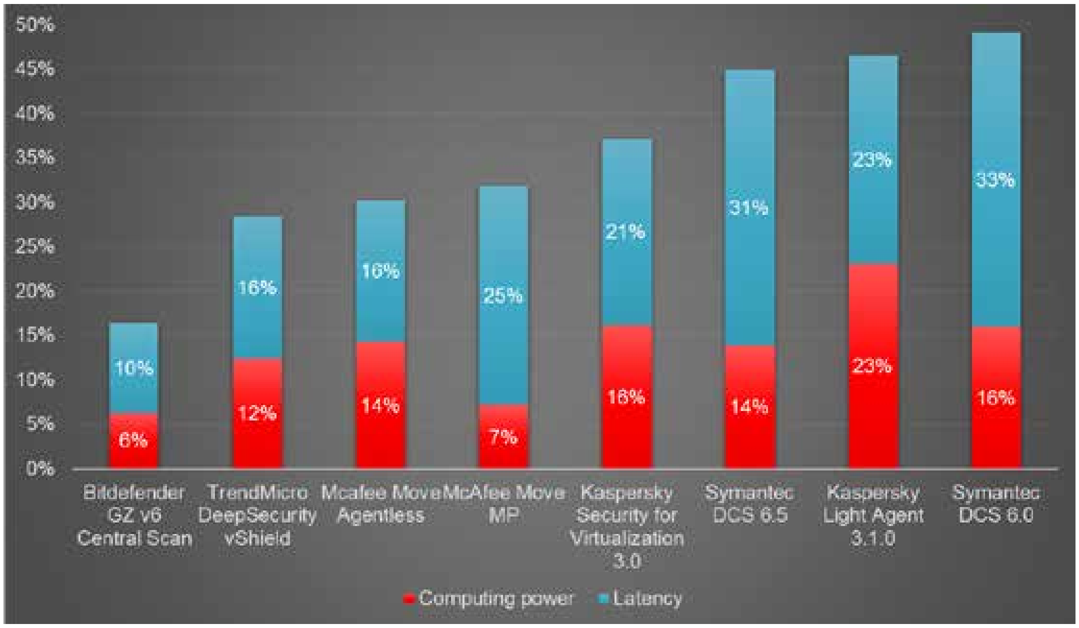


Figure 3: Antimalware impact on system load and latency

Since the overall picture relies on both VSImax and Baseline, the results have been combined in



In the figure, the latency is expressed as a percentage increase in Baseline over running the same test with no antimalware installed. The computing power is represented as a percentage increase in hardware load applied by each VDI instance by comparing VSImax of each solution against VSImax with no antimalware installed.

Conclusion

Without question, security is paramount to ensuring the security of data. However, security must not hamper the business in any way. Choosing the right security solution is the difference between a successful virtualization project, and additional capital outlay on more hardware, frustrated employees, and wasted productivity. In a VDI environment, the security solution implemented must have the least possible impact – shorter waiting times for applications to open results in better employee productivity and consequently in fewer helpdesk calls.

GravityZone Security for Virtualized Environments is an all-encompassing security solution, specifically built for any virtualized infrastructure. When SVE is deployed in a VDI environment, it supports the highest number of VDI sessions achievable compared to any other virtualization security solution available on the market. It also minimizes the impact in latency, while providing antimalware protection for files, memory, processes and registry.

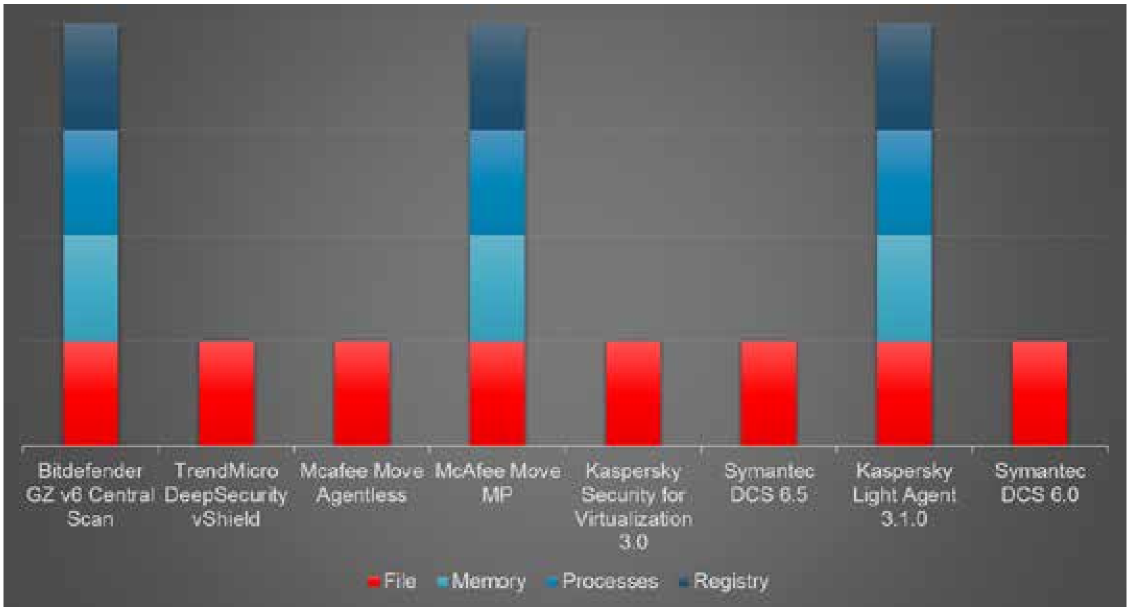


Figure 4: Scope of protection

When compared to other virtualization security solutions, using SVE in a VDI environment results in:

- Improved cost savings.
- Improved application response time.
- Increased number of VDI sessions.
- Flexibility of using any hypervisor.
- Comprehensive protection for files, memory, processes and registry.

Appendix

Testing methodology

All security solutions were installed and tested in minimum default installation with antivirus and antimalware features activated.

VSImax v4 (Max # of VDIs): VSImax v4 shows the number of concurrent sessions that can be active on a system before the system is saturated. This number gives you an indication of the scalability of the environment (higher is better).

VSIbase: VSIbase indicates the performance of the system while there is no load on the environment. This number is used to determine what the performance threshold will be. VSIbase gives an indication of the base performance of the environment (lower is better).

VSImax v4 Threshold: VSImax v4 threshold indicates the saturation point of the environment and is based on VSIbase. The threshold for the total response time is: average weighted baseline phase response time + 2600ms.

Calculating VSImax v4: The simulated desktop workload is scripted in 48-minute loops during which a simulated Login VSI user performs generic Office worker activities. Within each loop the response times of twelve specific operations are measured in a regular interval.

The response time of these actions are weighted before they are added to the total, so as to ensure that each activity has an equal impact on the total response time. Weighting applies as follows:

Activity	**Weight (%)**
Start VSI Notepad with large text file	50%
File Open Dialogue	125%
Start Print Dialogue	400%
Zip PST file without compression	600%
Zip PST file with high compression	17,5%
Start Word with new document	15%

1. VsiMax Dymanic (ms): The formula for the dynamic threshold is: Avg. Baseline Response Time x 125% + 3000. As a result, when the baseline response time is 1800, the VSImax threshold will now be 1800 x 125% + 3000 = 5250ms.

2. VsiMax # VDI: When the response (ms) of all the sessions is above VsiMax Dymanic (ms) the “Maximum number of logged on sessions” (VsiMax # VDI) has been reached “End of test”;

3. Number of machines: Before starting the actual tests, a number of VDIs are started waiting for Login VSI to login to the environment. 220 virtual machines are started at the beginning of each test run. This is performed to better mimic production environments where login may fail. Therefore, the number of “standby VDIs” is larger than the “logged on VDIs” and it has to be a constant value to make the test number of VDIs the same for all test runs.

4. Test Timeframe: The testing tool (Login VSI Tool) launches sessions, there has to be some delay between the launched sessions. This value is set before testing to calibrate Login VSI for the environment. The “Timeframe” value is the total time allocated for launching all 220 sessions. The testing tool will logon a user every 16 seconds. This means it must finish logging in all users within 3600 seconds.

5. Heavy workloads: The heavy workload utilizes higher memory and CPU consumption because more applications are running in the background. This workload simulated a power user. Once a session has been started the heavy workload will repeat every 12 minutes. During each operation the response time is measured every 2 minutes.

- The heavy workload opens up to 8 apps simultaneously.
- Type rate is 130ms per character.
- 40 seconds of Idle time to simulate real-world users.

- Each loop will open and use the following:
- Outlook 2007/2010, browse 10 messages.
- Internet Explorer, one instance is left open (BBC.co.uk), one instance browsers to Wired.com, Lonelyplanet.com and heavy flash app gettheglass.com.
- Word 2007/2010, one instance to measure response time, one instance to review and edit document.
- Bullzip PDF Printer & Acrobat Reader, the word document is printed and reviewed to PDF.
- Excel 2007/2010, a very large randomized sheet is opened.
- PowerPoint 2007/2010, a presentation is reviewed and edited.
- 7-zip: using the command line version the output of the session is zipped.

6. Testing environment description:

• vCenter	5.5.0 1476327
• VMware Tools	9.4.0, build-1280544
• VDI Manager VMware View	5.3.0 build 1427931
• vShield Manager	Release 5.5.3-217697
• Endpoint Driver	Version 5.1.0-01814505 (Mux Driver)

Host1 (Dell R710)5.5.0 1331820

• CPU	2 x Xeon E5645 @2.4 GHz
• RAM	128GB DDR3
• Storage Controller	Perc H700
• Disks	5 x OCZ Vertex 3 in Raid 0 Config
• Net	2 x Gigabit Ethernet

Host2 (Dell R710)5.5.0 1331820

• CPU	2 x Xeon E5645 @2.4 GHz
• RAM	128GB DDR3
• Storage Controller	Perc H700
• Disks	5 x OCZ Vertex 3 in Raid 0 Config
• Net	2 x Gigabit Ethernet

Testing policy:

- Scan all Files
- Scan network files
- Archives excluded from scanning
- Mail archives excluded from scanning
- Windows 7 X86 SP1, updated
- Defragmenter disabled
- Search indexer disabled
- Windows update disabled
- Scheduled tasks disabled
- Firewall disabled

- Windows defender disabled
- Web proxy auto-discovery disabled
- Themes disabled
- Superfetch disabled
- Application experience enabledabled
- Offline files disabled
- Security center disabled
- Machine debug manager disabled
- Error reporting disabled
- 1172 RAM allocated with no reservation
- 1 VCPU allocated with no reservation
- Pagefile set static to 2x RAM

Tested with Login VSI version 4.1.0 in April 2015

About Login VSI

Login VSI, Inc. delivers industry-standard testing solutions for virtualized desktop and server environments. The world's leading virtualization vendors use the flagship product, Login VSI, to benchmark the performance and scalability of their solutions. Enterprise IT departments use Login VSI in all phases of their virtual desktop deployment—from capacity planning, to load testing, to change impact prediction—for more predictable performance, higher availability and a more consistent end user experience. With minimal configuration, Login VSI works in VMware Horizon View, Citrix XenDesktop and XenApp, Microsoft Remote Desktop Services (Terminal Services) and any other Windows-based virtual desktop solution. For more information, download a trial at www.loginvsi.com.

BD-Business-May.13.2015-Tk#: 70767