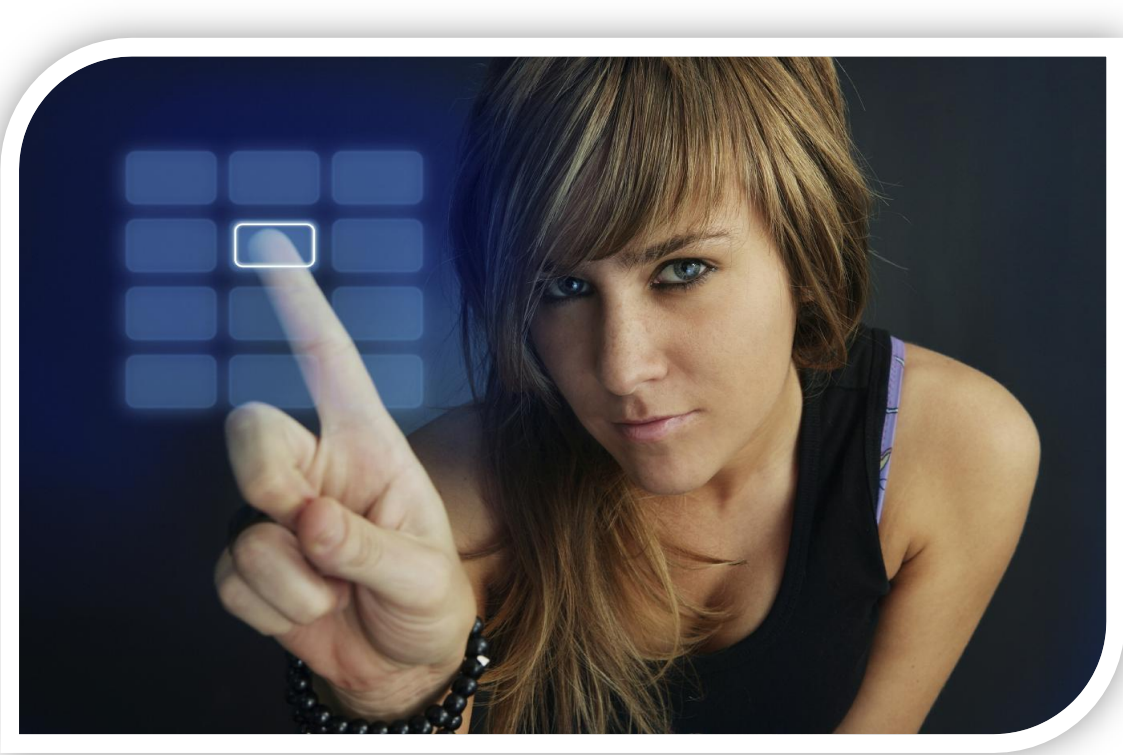
Virtual Reality Check



Project VRC: Phase V

Antivirus impact and best practices on VDI

Author(s) : Jeroen van de Kamp and Ruben Spruijt

Version: 1.02

Date: January 2013

Log.in consultants

PQR

Eenvoud in ICT

©2013 PQR and Login Consultants, all rights reserved.

All rights reserved. Specifications are subject to change without notice. PQR and Login Consultants, the PQR and Login Consultants logo and its tagline Eenvoud in ICT are trademarks or registered trademarks of PQR and Login Consultants in the Netherlands and/or other countries. All other brands or products mentioned in this document are trademarks or registered trademarks of their respective holders and should be treated as such.

CONTENT

1. Summary 3
2. Introduction 5
2.1 Tested solutions 6
2.2 Important disclaimer: VRC investigates performance impact only 8
3. Introduction to Project VRC 9
3.1 Project VRC objectives 9
3.2 Intended audience 10
3.3 Better together 10
3.4 Vendor involvement 10
3.5 Contact 10
4. About the authors 12
4.1 About Login Consultants 12
4.2 About PQR 12
4.3 Team members 13
4.4 Special thanks 14
5. The Login VSI benchmark 15
5.1 Login VSI overview 15
5.2 Login VSI 3.6 workload 16
5.3 What's new in Login VSI 3.6 17
5.4 VSImax 18
5.5 Calculating VSImax 19
5.6 Interpreting Project VRC results 22
6. The VRC platform 24
6.1 Hardware configuration 24
6.2 Launcher configuration 25
6.3 Test approach 25
7. Understanding Antivirus architectures 26
7.1 Conventional Antivirus architecture 26
7.2 Off-loading architectures 27
8. Testing Antivirus solutions 29
8.1 Stateful versus stateless 29
8.2 Default settings 29
8.3 The critical importance of an image Pre-Scan 30
8.4 Tuning the Antivirus agent for performance 33
9. McAfee VirusScan Enterprise 8.8.0 34

9.1 VSImax results 34
9.2 Baseline Login VSI response time results 35
9.3 Disk IO results 36
9.4 CPU utilization with 50 sessions 39
9.5 Overview of settings 41
10. McAfee MOVE Multiplatform 2.0 43
10.1 VSImax results 43
10.2 Baseline Login VSI response time results 44
10.3 Disk IO results 45
10.4 CPU utilization with 50 sessions 48
10.5 Overview of settings 49
11. McAfee MOVE Agentless 2.5 50
11.1 VSImax results 50
11.2 Baseline Login VSI response time results 51
11.3 Disk IO results 51
11.4 CPU utilization with 50 sessions 53
11.5 Overview of settings 54
12. Symantec Endpoint Protection 12.1 55
12.1 VSImax results 55
12.2 Baseline Login VSI response time results 56
12.3 Disk IO results 57
12.4 CPU utilization with 50 sessions 59
12.5 Overview of settings 61
13. Microsoft Forefront Endpoint Protection 2010 63
13.1 VSImax results 63
13.2 Baseline Login VSI response time results 64
13.3 Disk IO results 65
13.4 CPU utilization with 50 sessions 67
13.5 Overview of settings 69
14. Comparing default on VMware vSphere 71
14.1 VSImax comparisons vSphere 4.1 71
14.2 Baseline Login VSI response time comparisons vSphere 4.1 72
14.3 Disk IO total commands @ 50 sessions comparisons vSphere 4.1 73
14.4 Disk IO read commands @ 50 sessions comparisons vSphere 4.1 74
14.5 Disk IO write commands @ 50 sessions comparisons vSphere 4.1 76
14.6 CPU average utilization @ 50 sessions comparisons vSphere 4.1 76

1. SUMMARY

This whitepaper about the performance impact and best practices of antivirus (AV) solutions within VDI took a little more effort than expected (and that is an understatement). However, the outcome seems worth it. Testing AV solutions proved to be more complex and more unpredictable than originally expected. It became very clear that most AV solutions were designed for typical Desktop and Laptop environments, not for (stateless) hosted virtual desktop environments.

There is an important lesson to be learned here: the impact of antivirus is considerable, and it's vitally important to review and test this before rolling out an AV solution in a VDI environment. This is confirmed in the large majority of real-world VDI deployments, time and again.

The issues witnessed and sometimes unexplainable results, forced the project VRC team to completely re-evaluate their testing approach. This was done by reconfiguring the complete VRC lab and implementing a fully automated workflow: both for performing the tests and evaluating the data. As a result, this whitepaper contains more data from more different configurations than any previous publication.

The findings are sometimes a little surprising. A key outcome of this whitepaper is the best practice to perform a pre-scan of the master image before it's deployed. The effect is dramatic and therefore highly recommended. Many different performance optimizations were tested. However, many are also difficult to recommend because they lower the amount of security features and would result in objections from security officers. Luckily, performing a pre-scan of the master image would not cause objections.

Another key finding is that off-loading architectures make a big difference from a storage IO point of view, but not always from a session density point of view. In comparison to conventional AV solutions, off-loading AV architectures have clear advantages (such as minimizing scanning overhead, central updates and minimized footprint per desktop VM). Nonetheless, off-loading architectures still needs to mature: technically they can be complex. Off-loading architectures create a very high dependency of the desktop VM's to the performance of the off-loading VM itself, especially when the server host is close to saturation. Also, off-loading architectures sometimes introduces higher application start latency, because the actual scanning of files is performed on a different VM.

Overall, the capacity impact on session density of using AV solutions within VDI with default settings ranges from 5 to almost 40%. Such impact has been witnessed, even with scheduled updates and scans disabled, and full pre-scan performed of the master image. Still, in the real world the performance impact of AV solutions can be easily bigger for multiple reasons:

- The scheduled scan and updates are often not properly configured. These activities consume a lot of CPU but most importantly, dramatically increase disk IO. This is fine when it only happens in a single desktop VM, but can lead to serious performance issues when it happens in many desktop VM's simultaneously.
- Only 1% of the audience who attended the preview VRC presentations (more than 2000 attendees in 2012 so far) indicated they performed a pre-scan of the image before deployment. As a result, in the far majority of VDI deployments, the pre-scan is not a common best-practice.
- The dataset is reasonably limited with Login VSI 3.6: in the real world typical office users would surf many more websites, work with many more documents of all types and review many more emails. This data stream, which continuously needs to be scanned, is consistent, infinite and new every single day.

When comparing various AV solutions, the conventional Microsoft System Center Endpoint Protection (SCEP) previously known as Forefront, seems to have the least performance impact, but only after performing a full pre-scan of the master image before deployment of the desktop VM's. This is a huge difference to Forefront tests done without pre-scan of the master image (in those tests, without pre-scan, the performance impact was dramatically high)

It is important to highlight the fact that Project VRC does not evaluate quality of the security features in any way. While one AV solution might have a lower performance impact, it could easily also mean that this AV solution is less effective to its competitors. It is important to include this into your own discussion about AV within VDI. We also realize that in many VDI environment there is no choice and configuration freedom, because of security policies and / or decisions made outside the VDI team. It's therefore critically important to educate colleagues about the impact of AV on VDI - hopefully this whitepaper can help with that process!

2. INTRODUCTION

When virtual Windows desktops are hosted on shared hardware in the datacenter, it's important to care about performance and capacity. Because the hardware is shared by users, and the available resources are limited, sizing and user experience become important topics. The capacity of the hardware (server and storage) is always limited. Ultimately, this can have a significant impact in the business case of desktop virtualization. Relatively small differences of 10 or 20 percent in desktop capacity can significantly increase required investments.

The desktop virtualization industry is maturing: we learned about IOPS, we learned how to tune the Windows desktop and hypervisor for performance and now know how to create scalable solutions. Interestingly, once everything is up and running, in many VDI deployments one piece of the performance pie is still overlooked: the antivirus solution. Too many times, moving into production, performance is not as expected. Often in these cases, antivirus solutions prove to have a considerable impact.

This is logical because antivirus agents have intelligent filters that scan the system and user activity. They do this by scanning files on reads and writes, and actively monitoring process (e.g. internet explorer). Because viruses are getting smarter, so are the antivirus solutions.

"Traditionally, AV solutions have relied strongly on signature-based scanning, also referred to as scan string-based technologies. The signature-based scan engine searches within given files for the presence of certain strings (often also only in certain regions). If these predefined strings are found, certain actions like alarms can be triggered. Modern scan string-based engines also support wildcards within the scan strings, which e.g. makes the detection of slightly polymorphic malicious codes much easier. However, signature-based scanning only detects known malware and may not detect against new attack mechanisms.

Heuristic scanning is similar to signature scanning, except that instead of looking for specific signatures, heuristic scanning looks for certain instructions or commands within a program that are not found in typical application programs. As a result, a heuristic engine is able to detect potentially malicious functionality in new, previously unexamined, malicious functionality such as the replication mechanism of a virus, the distribution routine of a worm or the payload of a Trojan."

Source: http://www.symantec.com/connect/articles/heuristic-techniques-av-solutions-overview (Author Markus Schmall)

Technologies like heuristics scanning add considerable weight to the scanning process. Normally, with regular desktops or laptops, this is not a problem. There's plenty of CPU and disk I/O capacity available exclusively to the (PC of the) user. However with hosted desktops this is different. A performance impact of up to 40 percent is not unusual after AV is installed. While this has been less of an issue with PC's or laptops, with VDI

it means you need to invest in 40% additional server capacity, or even higher when you look at the impact on storage.

For this reason Project VRC decided to investigate the impact of antivirus solutions on VDI. The following questions were asked:

- What is the performance/capacity impact of the most well-known AV solutions when used in a VDI environment?
- How do AV solutions designed for virtual environments with so called "off-loading" architectures compare with conventional solutions from a performance perspective?
- How does the disk IO impact compare with the different AV solutions, conventional and off-loading architectures?
- What is the performance impact in stateless desktop environments in comparison to stateful desktops?
- What possibilities are there for performance tuning and how does this affect the overall impact on performance impact?

2.1 TESTED SOLUTIONS

The purpose of this paper is to find the answers to these questions. Because there are so many AV vendors Project VRC focuses on the most common ones:

Microsoft

- Forefront Endpoint Protection 2010 (Now System Center Endpoint Protection 2012)

McAfee

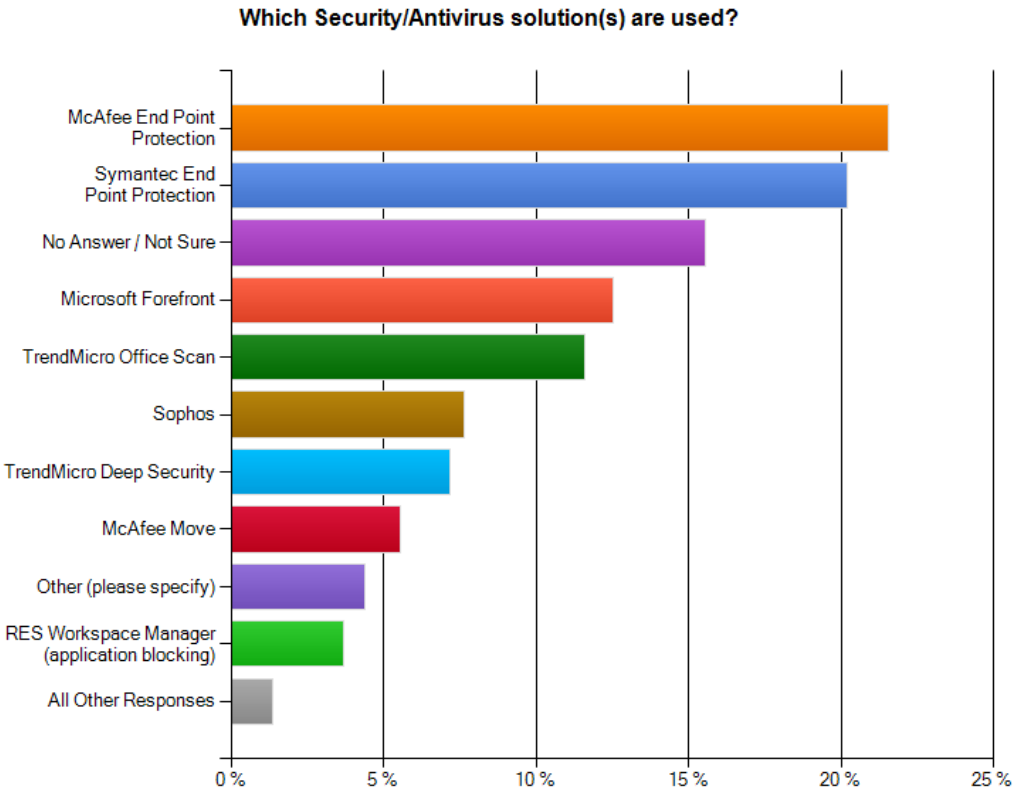
- Enterprise 8.8.0
- MOVE Multiplatform AV 2.x
- MOVE Agentless AV 2.5

Symantec

- Endpoint Protection 12.1

Project VRC started the first 'VRC state of the VDI & SBC union survey' in the fall of 2012. In this survey also was asked which AV solution(s) are used. Participants could select multiple AV & security solutions.

The full 'State of the Virtualization Union 2013 edition' will be available at www.projectvrc.com February 2013.


Which Security/Antivirus solution(s) are used?
McAfee End Point Protection
Symantec End Point Protection
No Answer / Not Sure
Microsoft Forefront
TrendMicro Office Scan
Sophos
TrendMicro Deep Security
McAfee Move
Other (please specify)
RES Workspace Manager (application blocking)
All Other Responses
0 %
5 %
10 %
15 %
20 %
25 %

2.2 IMPORTANT DISCLAIMER: VRC INVESTIGATES PERFORMANCE IMPACT ONLY

The results in this paper do no evaluate the quality of the AV solutions. Project VRC only investigates and compares the performance impact of the different solutions and configurations, including the performance impact of optimizations within these antivirus solutions. In addition, it is not Project VRC's aim to research the performance impact of (AV) maintenance: updating the AV database and performing a full system scan in the background. Because the (storage) impact is so substantial, it's always recommend to load balance/distribute such activities during maintenance hours.

Understand that real-world impact of AV solutions will probably be bigger than Project VRC reports. This is mostly because the dataset used within Login VSI is relatively small: 100 files per document type in the pool (pst, doc, ppt, etc..) are used within the test, a limited set of applications is used (mostly Microsoft Office and IE) and a limited amount of websites is visited. In the real-world, both the amount and diversity of data, the amount of applications and off course the amount of websites visited is far greater.

Lastly, this **project cannot and will not recommend any of the performance optimization being tested**, with a few exceptions that have no impact on the functionality of the antivirus agent. Many of the optimizations will reduce the functionality and security level of the AV solution, so everyone reading this document needs to evaluate and value all configurations and optimizations accordingly. Project VRC never recommends using a configuration that conflicts with corporate policy guidelines or common sense.

3. INTRODUCTION TO PROJECT VRC

Welcome to "Project: Virtual Reality Check (VRC)"!

If you're looking for independent advice and a 'Reality Check' in relation to virtualizing Terminal Server and desktop (VDI) workloads, if you are curious about the impact of different hypervisors and the performance differences with various hardware, if you're searching for best practices for your virtual desktops and if you're curious about the performance impact of different Application Virtualization and Antivirus Solutions within VDI … the different Project VRC whitepapers are a must read!

PQR and Login Consultants started this unbiased and independent R&D project early 2009. The goal of Project VRC is to analyze the developments in the Application- and Desktop Virtualization market and to objectively present the results. All together over 1500 tests have been carried out (Q4-2012).

In the haze of the extreme rate of innovation in the virtualization market and corresponding marketing promises this information is appreciated. Therefore we published our methods and conclusions in various whitepapers which can be downloaded from www.projectvrc.com

3.1 PROJECT VRC OBJECTIVES

The overall goal of Project VRC is to investigate, validate and give answers to the following questions and much more:

- What is the true impact of innovations on a hardware and hypervisor level?
- Which performance optimization on the host and guest virtualization level can be configured, and what is the impact of these settings on user density?
- With the introduction of the latest hypervisor technologies, can we now recommend running large scale TS/CTX workloads on a virtualization platform?
- How does a VDI infrastructure scale in comparison to Terminal Server?
- How do various Microsoft Windows Client OSes scale as a virtual desktop?
- How do x86 and x64 Terminal Server platforms compare in scalability on bare metal and in virtualized environments?
- What is the best way to partition (memory and vCPU) the Virtual Machines on the hypervisor host, to achieve the highest possible user density?
- What is the impact of the latest and greatest hardware on Terminal Server and VDI desktops?
- What is the impact of adding extra 'layers' to a Terminal Server or VDI desktop environment, like application virtualization?
- What is the impact of adding extra 'layers' to VDI desktops, like antivirus?

Project VRC is not finished, and probably never will be. We look forward to evaluate new innovations in the hypervisor arena, hardware level, Windows 8/Server2012 and

impact in VDI and Remoting Protocols. Project VRC publishes their findings on www.projectvrc.com.

3.2 Intended audience

This document is intended for IT Managers, Architects, (Performance) Analysts, System Administrators and IT-Pros in general who are responsible for and/or interested in designing, implementing and maintaining virtualized Terminal Server and Virtual Desktop Infrastructures.

3.3 Better together

"...The two largest and most focused competitors in the Dutch Virtualization, Application Delivery and Enterprise Mobility market space are working together on Project Virtual Reality Check..." PQR and Login Consultants started this joined-venture to share insights with the virtualization community with Project Virtual Reality Check (Project VRC). There are several reasons for PQR and Login Consultants to execute this project together:

- The Project leaders, Ruben Spruijt and Jeroen van de Kamp have known each other for a long time from the virtualization community and share the same passion for these technologies.
- Project VRC is a huge undertaking, PQR and Login Consultants individually do not have the resources, or time, to execute this project on their own. Thus is it logical to cooperate, share the workload and deliver the results together.
- Both organizations share the same technical vision, which is critically important in complicated projects like these.

3.4 Vendor involvement

All major vendors whose products are covered by Project Virtual Reality Check, such as McAfee, Microsoft and Symantec have been approached in advance to create awareness of Project VRC and discuss the results.

3.5 Contact

All information about Project Virtual Reality Check can be found at www.projectvrc.com. Contact details of the participating organizations are:

PQR
Tel: +31 (0)30 6629729
E-mail: info@pqr.nl
www.pqr.com

Login Consultants
Tel: +31 (0)20 3420280
E-mail: info@loginconsultants.nl
www.loginconsultants.com

We try to provide accurate, clear, complete and usable information. We appreciate your feedback. If you have any comments, corrections, or suggestions for

improvements of this document, we want to hear from you! Please send an email to Jeroen van de Kamp (j.kamp@loginconsultants.nl) or Ruben Spruijt (rsp@pqr.nl). Please include the title of the document, the version number, and the page that you refer to, in your message.

THIS DOCUMENT IS PROVIDED "AS IS"

WITHOUT WARRANTY OF ANY KIND

FOR REFERENCE PURPOSES ONLY

COPYRIGHT 2013, PQR & LOGIN CONSULTANTS

IT IS NOT ALLOWED TO (PARTIALLY) PUBLISH OR DISTRIBUTE CONTENT FROM THIS PAPER WITHOUT PRIOR APPROVAL

4. ABOUT THE AUTHORS

4.1 ABOUT LOGIN CONSULTANTS

Innovations of the desktop infrastructure bring significant benefits in the areas of cost, security, and user experience. The challenge is to find the perfect balance between end-user freedom and manageability. Exponential growth of possibilities when it comes to devices, virtualization technologies, application models and cloud solutions make it difficult to keep an eye on the ball.

Login Consultants is an independent international IT service provider specialized in End User Computing. We help our clients in finding the optimal balance between IT control and end user flexibility. Our goal is create innovative solutions which simplify future change. Our success with our customers is built on the quality of integration combined with a smart migration approach and the manageability of the solution after deployment.

Login Consultants has an experienced team with over 140 consultants in The Netherlands, Belgium and Germany. Our consultants have accreditations from Microsoft, Citrix and VMware, and are regularly invited to speak at national and international events. They are involved as experts in online and printed IT publications and actively participate in relevant technical blogs.

Login Consultants' innovative drive is materialized in our own Solutions-lab. The specialists of Login Consultants continuously create innovative software solutions to support and enhance the quality of centralized desktop implementations. These efforts resulted in a suite of software tools adding value to the software solutions of Citrix, Microsoft, VMware and others. These freeware tools are used and appreciated by thousands of companies worldwide. The Solution-lab of Login Consultants has been the incubator for successful software solutions, like Flex Profiles, Login VSI and Automation Machine for Hosted Desktops.

4.2 ABOUT PQR

PQR is the professional ICT infrastructure specialist focusing on the availability of data, applications and work spaces with optimized user experience in a secure and manageable way.

PQR provides its customers innovative ICT solutions, from on-premise to cloud management, without processes getting complex. Simplicity in ICT, that's what PQR stands for.

PQR has traceable references and a wide range of expertise in the field, proven by many of our high partner statuses and certifications. PQR is Citrix Platinum Solution Advisor, HDS Tier 1 Platinum Partner, HP GOLD Preferred Partner, Microsoft Gold Partner, NetApp Star Partner, RES Platinum Reseller, VMware Premier Partner en VMware Gold Authorized Consultant Partner.

PQR's approach is based on four main pillars:

- Data & System Availability
- Application & Desktop Delivery
- Secure Access & Secure Networking
- Advanced IT Infrastructure & (Cloud) Management

PQR, founded in 1990, is headquartered in De Meern and counts over 107 employees. In fiscal year 2011/2012 posted sales of € 94.9 million and a net after tax profit of € 4.6 million have been recorded.

4.3 TEAM MEMBERS

Sven Huisman, Consultant @ PQR

Sven Huisman (1977) studied Information Management in Utrecht. He started his career as system engineer and meanwhile he has over 10 years of experience in the IT business. He is one of PQR's technical consultants, focusing on Application and Desktop Delivery, hardware and software virtualization. Sven advises, designs, implements and migrates advanced ICT-infrastructures. He is a Citrix Certified Enterprise Administrator (CCEA), a Microsoft Certified Systems Engineer (MCSE) and a VMware Certified Professional (VCP). Sven is blogging about virtualization on VirtualFuture.info and was awarded as VMware vExpert. To contact Sven directly send an email to shu@pqr.nl. Follow Sven on twitter.

Dennis Geerlings, Consultant @ Login VSI

Dennis started at Login VSI about 2.5 years ago and worked as consultant within Login Consultants. He supported multiple customers in migration projects. Right now Dennis is support manager and lead consultant at Login VSI. In these roles he supports customers and partners, co-develops the Login VSI solution and acts as pre-sales for enterprise customers. Dennis has performed most of the tests for this whitepaper and created the test and analysis automation process in the Project VRC labs. Dennis is the main technical contact for customers and partners in the United States and Canada. To contact Dennis directly send an email to d.geerlings@loginvsi.com

Jeroen van de Kamp, CTO @ Login Consultants

As Chief Technology Officer, Jeroen van de Kamp (1972) is responsible for defining and executing the technical strategy for Login Consultants. From the start, Jeroen has played a critical role in the technical growth and accreditation Login has accumulated over the years. He has developed several core solutions which allow Login Consultants to easily differentiate themselves in the infrastructure consulting market.

Jeroen is also responsible for several well-known publications like the Flex Profile Kit, TCT templates & "The black hole effect". Because of his contribution to the technical community van de Kamp is recognized as a thought-leader in the application delivery industry and has become a residential speaker for seminars like BriForum, Citrix

Solution Summit and many others. He is one of the 25 members worldwide who participate in the exclusive "Citrix Technology Professional" program. Jeroen is still engaged with strategic key accounts for Login Consultants, defining and realizing all-encompassing strategies for complex application, desktop and server delivery infrastructures. Previous to his position as CTO at Login Consultants Jeroen held positions as Infrastructure Architect at Login Consultants; as IT Consultant at QFace ICT and as IT specialist at ASG de Veer. To contact Jeroen directly send an email to j.vandekamp@loginconsultants.nl or follow him on twitter: @thejeroen.

Ruben Spruijt, CTO @ PQR

Ruben Spruijt (1975) is CTO and focuses primarily on Enterprise Mobility, Virtualization and Cloud Management. He is actively involved in determining PQR's vision and strategy.

Ruben is Microsoft Most Valuable Professional (MVP), Citrix Technology Professional (CTP) and VMware vExpert and is the only European with these three virtualization awards. He gives customers advice and has them benefit from his expertise; he motivates his colleagues and writes blogs, articles and opinion pieces on a regular basis. During presentations in several national and international congresses, Ruben shares his thoughts and knowledge on application and desktop delivery, and on virtualization solutions.

To contact Ruben directly send an email to rsp@pqr.nl. Follow Ruben on twitter: @rspruijt .

4.4 SPECIAL THANKS

A lot of effort has been put into this paper by many.

Project VRC wants to specifically thank **Jonathan Meunier**, who was a VRC team member in 2011 and performed the first tests for this AV whitepaper.

Also, special thanks **Alistair Gillespie**, who reviewed this publication and helped to improve its content in many ways. Great work!

5. THE LOGIN VSI BENCHMARK

For Project VRC, the industry standard Login Virtual Session Indexer (Login VSI 3.6) benchmarking solution was used. Login VSI offers a benchmarking methodology which calculates index numbers based on the amount of simultaneous sessions that can be run on a single physical machine, running either bare metal or virtualized operating systems. The commercial version of Login VSI offers different pre-packaged workloads and workload customization, including the addition of customer specific applications.

To keep the results of the Project VRC tests representative it is imperative that 100% identical tests are run on different types of systems. Therefore, Project VRC uses the standard medium Login VSI workload without any customization of the load scripts.

Login VSI is used by many other companies to review performance and publish white-papers including: AppSense, Atlantis Computing, Bitdefender, Cisco, Citrix, Datacore Software, Dell, EMC, ESG, Gridcentric, Hitachi, HP, McAfee, Microsoft, Miercom, Principled Technologies and VMware. Many of these publications are listed here: http://www.loginvsi.com/white-papers

Login VSI focuses on how many users can run simultaneously on a system, while maintaining acceptable response times. Login VSI is comparable to investigating the maximum amount of seats on a bus or airplane using trial and error. This maximum number is called the “Virtual Session Index (VSImax)”.

On Virtual Desktop Infrastructure (VDI) and Server Based Computing (SBC) with Remote Desktop Services (RDS) workloads this gives very valid and useful information. This index simplifies comparisons and makes it possible to understand the true impact of configuration changes on hypervisor host or guest level.

Login VSI is a product independent benchmark which is specifically designed for VDI and SBC environments. With Login VSI it is possible to perform different load test scenarios:

- Test the maximum active session/desktop capacity (VSImax) of a single server
- Perform a stability/soak/stress test for a longer period on a single server
- Determine the maximum active session/desktop capacity (VSImax) of a group of servers (a site/block/farm/enclosure)
- Perform a stability/soak/stress test for a longer period on a group of servers (a site/block/farm/enclosure)

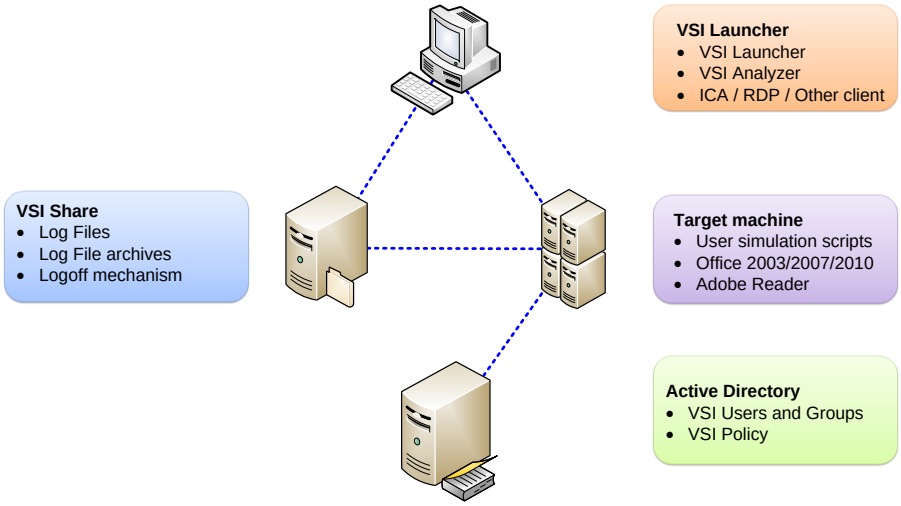
Login Virtual Session Indexer can be downloaded from: www.loginvsi.com

5.1 LOGIN VSI OVERVIEW

Login VSI 3.6 consists of 4 components:

- Active Directory Domain Controller for user accounts and standard policies

- A file share for central configuration and logging
- Launcher workstations (Master and Slaves) to initiate the sessions
- Target platform (VDI or SBC) where the user load scripts are installed and performed



5.2 LOGIN VSI 3.6 WORKLOAD

The standard (medium) Login VSI workload is the only workload available in Login VSI Express and is also available in Login VSI Pro.

- This workload emulates a medium knowledge worker using Office, IE, PDF and Java/FreeMind.
- Once a session has been started the medium workload will repeat (loop) every 14 minutes.
- During each loop the response time is measured every 2-3 minutes.
- The medium workload opens up to 5 applications simultaneously.
- The keyboard type rate is 160 millisecond for each character.
- Approximately 3 minutes of idle time is included to simulate real-world users.

Each loop will open and use:

- Outlook 2007, browse 10 messages.
- Internet Explorer, one instance is left open (BBC.co.uk), one instance is browsing to Wired.com, Lonelyplanet.com and a YouTube style video (480p movie trailer) is opened once every two loops.
- Word 2007, one instance to measure response time, one instance to review and edit a document.

- Bullzip PDF Printer & Acrobat Reader, the word document is printed and reviewed to PDF.
- Excel 2007, a very large randomized sheet is opened.
- PowerPoint 2007, a presentation is reviewed and edited.
- Freemind, a Java based Mind Mapping application is opened and viewed.

5.3 WHAT'S NEW IN LOGIN VSI 3.6

While the Project VRC phase I whitepaper is based on results from Login VSI 1.x, phase II is based on Login VSI 2.x, phases III and IV are based on Login VSI 3.x, this paper is based on results from Login VSI 3.6. What's new and different in version 3.6?:

Updated standard medium workload, based on the original medium workload:

- Alternating between 2 medium workloads: one with Flash video, one without. Once a workload is finished, the other type will start, all throughout the test.
- The flash app GetTheGlass is replaced by the "Kick-Ass" 480p movie trailer in flash format (.flv)
- Random start delay of max 15 seconds, to prevent workload synchronization
- Automatic loop length adjustments: when the load is higher, normally the total loop length increases: now automatically the pauses are decreased so the total loop length stays the same, even when the system approaches saturation.
- FreeMind (an open source JAVA application) is added to the medium workload.

Updated the light, heavy & multimedia workloads to include the same changes.

Completely revised logging structure:

- No more VSI_Log.xxxx, but SESSIONNUMBER_USERNAME_COMPUTERNAME.log
- The Log files are now using comma delimited CSV formatting
- Log files are now stored in VSI Share\ActiveTestName\Results
- Active sessions are not based on sessions launched, but truly active (logged on) sessions

Completely new analyzer, based on the MSchart add-on for .Net 3.5 sp1

- Fully automatic analysis (including stuck sessions)
- Dynamic charting (right click on the chart to set axis)
- Result selection and highlighting (similar to Windows Perfmon: right click in the lower window)
- Detailed charting

- Export Chart to PNG (other formats will follow)
- Local Access database to cache analysis

The highest and lowest scores: the 2% top and bottom results will be removed from VSImax calculation to reduce noise in the results.

5.4 VSIMAX

The philosophy behind Login VSI is different to conventional benchmarks. In general, most system benchmarks are steady state benchmarks. These benchmarks execute one or multiple processes, and the measured execution time is the outcome of the test. Simply put: the faster the execution time or the bigger the throughput, the faster the system is according to the benchmark.

Login VSI is different in approach. Login VSI is not primarily designed to be a steady state benchmark (however, if you wish, Login VSI can act like one). Login VSI was designed to perform benchmarks for SBC or VDI workloads through saturation. Login VSI loads the system with simulated user workloads using well known desktop applications like Microsoft Office, Internet Explorer and Adobe PDF reader. By gradually increasing the amount of simulated users, the system will eventually be saturated. Only by overloading a system it is possible to find out what its true maximum desktop capacity is.

After a test is performed, the response times can be analyzed to calculate the maximum active session/desktop capacity. Within Login VSI this is calculated as VSImax. If the system was not saturated during the test, it will not be able to calculate VSImax. However, when the system was saturated during the test, it is possible to determine the maximum capacity.

This VSImax is the “Virtual Session Index (VSI)”. With Virtual Desktop Infrastructure (VDI) and Terminal Services (TS) workloads this is very valid and useful information. This index simplifies comparisons and makes it possible to understand the true impact of configuration changes on hypervisor host or guest level.

5.4.1 Server side response time measurements

It is important to understand why specific Login VSI design choices have been made. An important design choice is to execute the workload directly on the target system within the session instead of using remote sessions. The scripts simulating the workloads are performed as a compiled AutoIT script on every target system, and are initiated at logon within the simulated user’s desktop session context.

An alternative to the Login VSI method would be to generate user actions client side through the remoting protocol. Remoting protocols like Microsoft RDP and Citrix ICA/HDX support this. However, such solutions are complicated to build and maintain. These methods are never product and vendor independent. With every change on a protocol level or with every new remoting solution, Login VSI would need to be

revised/expanded to support these changes. Even with a huge development budget, it is practically impossible to support every single remoting protocol. More importantly, some protocols simply do not have a method to script user actions at the client side.

For Login VSI a decision was made to execute the scripts completely server side with AutoIT. This is the only practical and platform independent solution, for a benchmark like Login VSI. The relative overhead and footprint of AutoIT is small enough (1-5% range) for Login VSI's purposes.

5.5 CALCULATING VSIMAX

Typically the desktop workload is scripted in a 12-14 minute loop when a simulated Login VSI user is logged on. After the loop is finished it will restart automatically. Within each loop the response times of seven specific operations is measured in a regular interval: six times in within each loop. The response times of these seven operations are used to determine VSImax.

The seven operations for which the response times are measured, are:

- **Copy new doc from the document pool in the home drive**

  This operation will refresh a new document to be used for measuring the response time. This activity is mostly a file-system operation.

- **Starting Microsoft Word with a document**

  This operation will measure the responsiveness of the Operating System and the file system. Microsoft Word is started and loaded into memory, also the new document is automatically loaded into Microsoft Word. When the disk IO is extensive or even saturated, this will impact the file open dialogue considerably.

- **Starting the "File Open" dialogue**

  This operation is handled for a small part by Word and a large part by the operating system. The file open dialogue uses generic subsystems and interface components of the OS. The OS provides the contents of this dialogue.

- **Starting "Notepad"**

  This operation is handled by the OS (loading and initiating Notepad.exe) and by the Notepad.exe itself through execution. This operation seems instant from an end-user's point of view.

- **Starting the "Print" dialogue**

  This operation is handled for a large part by the OS subsystems, as the print dialogue is provided by the OS. This dialogue loads the print-subsystem and the drivers of the selected printer. As a result, this dialogue is also dependent on disk performance.

- **Starting the "Search and Replace" dialogue**

  This operation is handled within the application completely; the presentation of the dialogue is almost instant. Serious bottlenecks on application level will impact the speed of this dialogue.

- **Compress the document into a zip file with 7-zip command line**

  This operation is handled by the command line version of 7-zip. The compression will very briefly spike CPU and disk IO.

These measured operations with Login VSI do hit considerably different subsystems such as CPU (user and kernel), Memory, Disk, the OS in general, the application itself, print, GDI, etc. These operations are specifically short by nature. When such operations are consistently long, the system is saturated because of excessive queuing on any kind of resource. As a result, the average response times will escalate. This effect is clearly noticeable to end-users. If such operations consistently consume multiple seconds the user will regard the system as slow and unresponsive.

With the release of Login VSI 3.6 it became possible to choose between 'VSImax Classic' and 'VSImax Dynamic'.

5.5.1 VSImax Classic

VSImax Classic is based on the previous versions of Login VSI, and is achieved when the average Login VSI response time is higher than a fixed threshold of 4000ms. This method proves to be reliable when no antivirus or application virtualization is used.

To calculate the response times the seven activities listed in the previous section are totaled. To balance these measurements they are weighted before they are summed. Without weighting individual response times before they are totaled, one specific measurement (out of seven) could dominate the results.

Within 'VSImax Classic' two measurements are weighted before they are added to the total VSImax response time:

- 'Starting Microsoft Word with a document' is divided by two (50%)
- 'Starting the "Search and Replace" dialogue' is multiplied by five (500%)

A sample of the VSImax Classic response time calculation is displayed below:

Activity (RowName)	Result (ms)	Weight (%)	Weighted Result (ms)
Refresh document (RFS)	160	100%	160
Start Word with new doc (LOAD)	1400	50%	700
File Open Dialogue (OPEN)	350	100%	350
Start Notepad (NOTEPAD)	50	100%	50

Print Dialogue (PRINT)	220	100%	220
Replace Dialogue (FIND)	10	500%	50
Zip documents (ZIP)	130	100%	130
	VSImax Classic Response Time		**1660**

The average VSImax response time is calculated based on the amount of active Login VSI users logged on to the system. When the average VSImax response times are consistently higher than the default threshold of 4000ms, VSImax is achieved.

In practice however, tests have shown a substantial increase of application response time when antivirus and/or application virtualization is used. The baseline response time is typically around 1400 - 1800 ms without application virtualization or antivirus. However, when antivirus or application virtualization is used, the typical baseline response time varies between 2500 – 3500 ms.

When the baseline response time is already this high the VSImax Classic threshold of 4000ms is very easily reached. 'VSImax Classic' will report its maximum value, long before relevant system resources like CPU, RAM or disk are actually saturated.

In Login VSI 3.6 'VSImax Dynamic' has been introduced to be able to support the wildly varying baseline response times that can be found in situations where antivirus and/or application virtualization is used.

5.5.2 VSImax Dynamic

Similar to 'VSImax Classic', VSImax Dynamic is calculated when the response times are consistently above a certain threshold. However, this threshold is now dynamically calculated on the baseline response time of the test.

Five individual measurements are weighted to better support this approach:

- Copy new doc from the document pool in the home drive: 100%
- Microsoft Word with a document: 33.3%
- Starting the "File Open" dialogue: 100%
- Starting "Notepad": 300%
- Starting the "Print" dialogue: 200%
- Starting the "Search and Replace" dialogue: 400%
- Compress the document into a zip file with 7-zip command line: 200%

A sample of the VSImax Dynamic response time calculation is displayed below:

Activity (RowName)	Result (ms)	Weight (%)	Weighted Result (ms)
Refresh document (RFS)	160	100%	160
Start Word with new doc (LOAD)	1400	33.3%	467
File Open Dialogue (OPEN)	350	100%	350
Start Notepad (NOTEPAD)	50	300%	150
Print Dialogue (PRINT)	220	200%	440
Replace Dialogue (FIND)	10	400%	40
Zip documents (ZIP)	130	200%	230
	VSImax Dynamic Response Time		**1837**

The average VSImax response time is calculated based on the amount of active Login VSI users logged on to the system. For this the average VSImax response times need to consistently higher than a dynamically calculated threshold. To determine this dynamic threshold, first the average baseline response time is calculated. This is done by averaging the baseline response time of the first 15 Login VSI users on the system.

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

Especially when application virtualization is used, the baseline response time can wildly vary per vendor and streaming strategy. Therefore it is recommended to use VSImax Dynamic when comparisons are made with application virtualization or antivirus agents. The resulting VSImax Dynamic scores are aligned with saturation on a CPU, Memory or Disk level, also when the baseline response time are relatively high.

5.6 Interpreting Project VRC results

Project VRC uses the product independent Login VSI 3.6 benchmark to review, compare and analyze desktop workloads on Terminal Server (TS) and VDI solutions. The primary purpose of VSImax is to allow sensible and easy to understand comparisons between different configurations.

The data found within Project VRC is therefore only representative for the VDI & TS workloads. Project VRC results cannot and should never be translated into any other workloads like Exchange, SQL, IIS, Linux, Unix, Domain Controllers etc…

Also, the “VSImax” results (the maximum amount of Login VSI users), should never be directly interpreted as real-world results. The Login VSI workload has been made as realistic as possible, but, it always remains a synthetic benchmark with a specific desktop workload. Real world TS and VDI performance is completely dependent on the specific application set and how these applications are used by the users. To include specific applications or to customize workloads, Login VSI Pro can be used.

6. THE VRC PLATFORM

Login Consultants and PQR built the benchmark platform for Project VRC at PQR in de Meern, The Netherlands. Login VSI 3.6 was used to create transparent, reproducible and stable performance tests on Server Based Computing (SBC) and Virtual Desktop (VDI) workloads. To effectively demonstrate the scalability of the Hypervisor platforms the benchmark environment has been built with the latest hardware- and software technologies. The focus in this whitepaper is to investigate the impact of antivirus solutions in Virtual Desktop (VDI) scenario's. For the tests in this whitepaper vSphere 4.1 and 5.0 are used, unless specifically stated otherwise. To perform image deployment in the different VDI tests scenarios VMware View 5 is used and RDP is used to connect to the desktop.

6.1 HARDWARE CONFIGURATION

All tests were performed on the following **HP Proliant** server hardware:

Component	Details
Server Brand/Model	HPDL380G6
BIOS version	P62 07/24/2009
CPU	2 x Intel Quad core x5550@2.67GHz
CPU cache	1MB L2, 8MB L3
Memory	96GB; 1333MHz
Disk	8 x 146GB, 820.2GB, dual port 10.000RPM Serial SCSI
RAID level	RAID-5 with online spare (25% Read / 75% Write)
RAID controller	HP Smart Array P400i, with 512MB and Battery Backed Write Cache
RAID controller	Firmware v5.20
Integrated Lights-Out (iLO) v2	Firmware v1.79
Network Interface	NetXtreme II

6.2 LAUNCHER CONFIGURATION

All the Login VSI launchers are installed and configured within Virtual Machines which are running on VMware. All the Login VSI launchers have been installed on Windows Server 2008 x86 Enterprise Edition SP2 with 2vCPU and 3GB memory. The Microsoft Remote Desktop Client (v6.0.6001) is included in the OS, no special configuration settings are applied. The VMware View 4.5 client was used for this AV whitepaper.

The RDP connection to the target machines was set to:

- 1024x786 Resolution
- 16 Bit Color Depth
- Speed Screen accelerators are disabled
- Client Drives are disabled
- Client Printing is disabled
- Clear Type is not configured

6.3 TEST APPROACH

Unless mentioned otherwise, Project VRC consistently used these methodologies to perform their tests:

- All test operations are fully automated: this ensures the consistency of the data.
- All tests are performed in a stateful and stateless desktop VM configuration.
- Before each test is started, the server host and launcher infrastructure are completely restarted to ensure the test is not influenced by previous tests.
- In all tests the VMs are pre-booted, as a result the logon interval is always 30 seconds.
- To ensure vSphere's Transparent Page Sharing (TPS) can free memory resources, each test is initiated at least 20 minutes after the last VM has been started.
- All tests are performed at least five times and the average result is reported in this document (both IO and VSImax).
- All VSImax tests are performed with ESXTOP running in the background with a 30 second interval.
- All tests are performed using local storage.
- VMware View Composer is used to create and deploy the VMs as linked clones.

Windows 7 was configured with 1GB memory. Windows 7 has roughly 600-700MB free memory available, which is more than enough for the Login VSI workload.

7. UNDERSTANDING ANTIVIRUS ARCHITECTURES

Some AV vendors have understood the potential overhead that comes with traditional antivirus architectures. When running 100 desktop VMs on a server, within each VM an AV agent is running. This agent is actively scanning files, registry and processes to find malware or viruses. Much of the data is the same for each desktop VM and user. However, the hardware: CPU, memory and storage is shared. Given this, it's possible to argue the architecture (where every VM runs its own agent independently) is quite inefficient.

This is the reason so called "off-loading" AV architectures were developed. Although technically there are some differences they all use the same principle: AV scanning is offloaded to a dedicated VM. As a result, a central database is updated with files and objects that have already been scanned and which can be regarded as safe. When other VMs access these files they're already flagged as safe and do not need to be scanned again.

In addition, the agent within each VM can be much smaller. Most scanning logic and the database do not have to be stored and executed within each VM. In an offloading architecture the footprint (both from a CPU, memory and storage point of view) of the AV agent in each desktop VM should be considerably smaller.

7.1 CONVENTIONAL ANTIVIRUS ARCHITECTURE

The conventional deployment architecture for antivirus solutions is the most simple. Within VDI it means that the AV agent is installed within the image, and then the master image is used to clone Desktop VM's in the desktop pool. The AV agents are centrally managed through group policies or the agents self-register (or are predefined) with a central management server.

In this model all AV scanning is done within each desktop autonomously and there is no information shared or offloaded to other VM's.

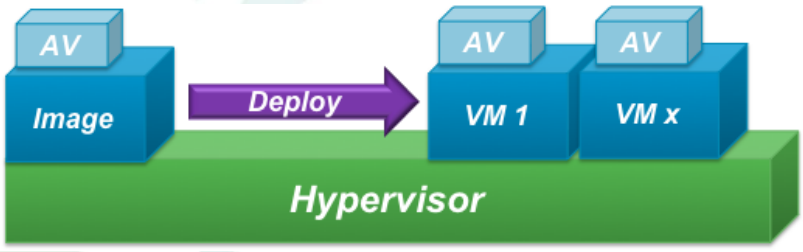


Figure 7-1 Conventional AV Deployment Architecture

This methodology is preferred and used with conventional AV solutions when it was technically possible. It is the fastest way to deploy the AV agents and only with this

model it is possible to perform a full system scan within the master image before it is cloned.

In practice this model can also cause issues. Especially when the central management server is not aware that for instance VM are redeployed to test a different configuration or when the (stateless) VM's are reset between tests. Most AV solutions require tuning or workarounds to prevent issues with the central management server, it is a clear indication that the conventional solutions are originally not designed to be used in (especially stateless) VDI environments.

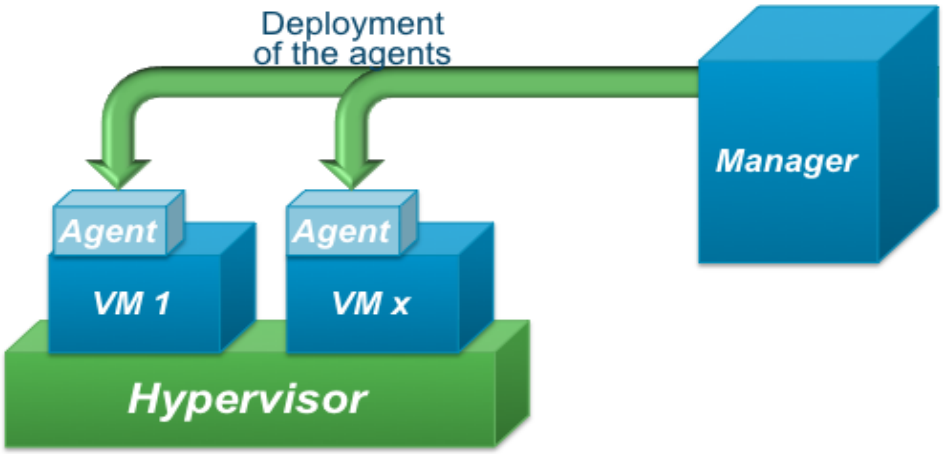


Figure 7-2 Deployment though central server

Technically it is also possible to deploy the AV agent through a central management server directly on the desktops in the pool, after the pool was created. This scenario works much better within a traditional Laptop and PC environment. In smaller stateful VDI environments this could also be practical. For project VRC this was clearly not the preferred deployment model, as it does not allow a pre-scan of the master image and is unworkable with a truly stateless configuration.

7.2 OFF-LOADING ARCHITECTURES

With a conventional antivirus solution the overhead can be considerable. Although the hardware is shared, every desktop VM includes a fully functional AV agent scanning the system and data independently of other agents. To address this overhead so called 'off-loading' AV architectures are getting more popular.

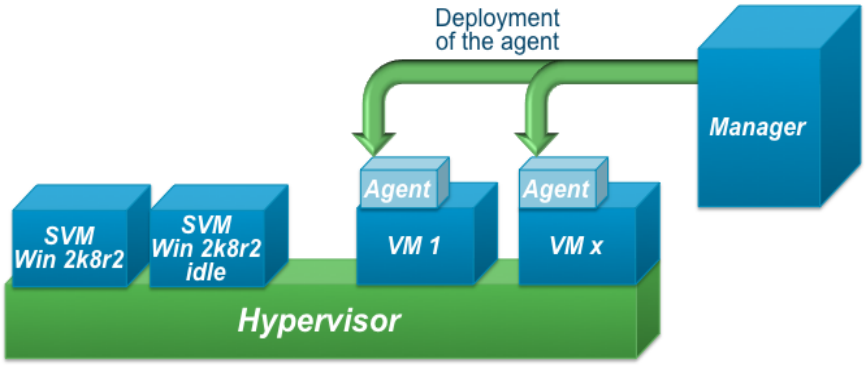


Figure 7-3 2.0 Example of the McAfee MOVE 2.0 off-loading architecture

The concept of an off loading architecture is simple: all actual scanning is performed by a dedicated VM. This VM retains a database of all scanned files, data and objects and flags these as 'safe'. The agent in the desktop VM has a very small footprint and only needs to forward the file to the off-loading VM if it is unknown and needs to be scanned first.

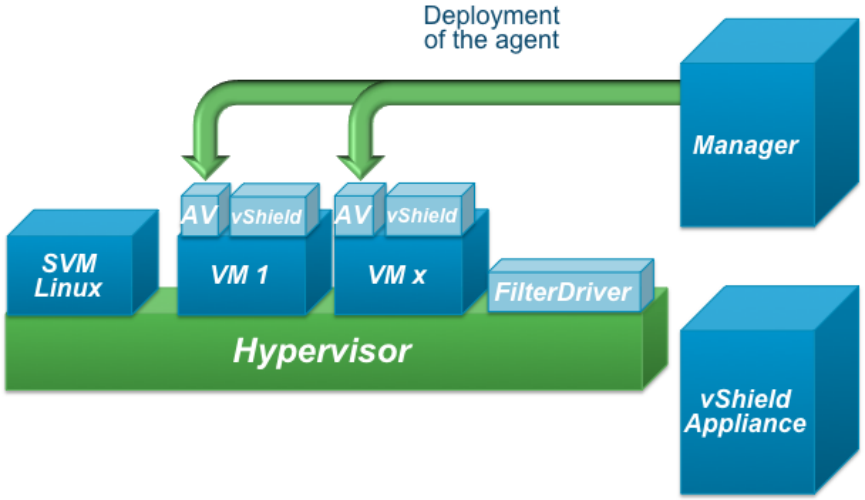


Figure 7-4 Example of the McAfee MOVE 2.5 off-loading architecture

There are two methods of off-loading. The communication between the AV agent and Scanning VM can either happen through the network, or through the hypervisor. The advantage of scanning through the network is that the off-loading VM can run on a physically different server. The advantage of communicating through the hypervisor is that it can be potentially more efficient and the footprint of the AV agent can even be smaller, as most logic and intercepts happen on a hypervisor level.

8. TESTING ANTIVIRUS SOLUTIONS

Some additional explanation is required to better understand how the tests are performed.

8.1 STATEFUL VERSUS STATELESS

As you might already know: hosted VDI is possible in two possible modes: 'stateful' and 'stateless'. A stateful desktop VM is not reset after it is used. Of course this model is used to provide personal desktops to end-users, as they always log in to their own machine. Then there is the 'stateless' VM model. There are many interpretations to what stateless means (just the fact that desktop pool is shared makes the VM stateless from a user perspective), but for Project VRC it means the VM is truly stateless and reset before it accepts a new user session.

Most tests are replicated for both the stateful and stateless desktop. There should be a considerable performance difference for a stateless desktop:

- In a stateful environment files are normally scanned on read only once, and then flagged as safe in the local AV database that is stored within the VM. This is typically done using a hashing algorithm. During the next test the file will be skipped when it is read, because its identity is known and flagged safe in the previous test. In a stateless VDI environment, hashing databases used by the AV agent are reset to the state it had within the golden image, before each test. As a result, when a file is scanned the AV agent will check its database, now this database is reset, this will happen within each test. This creates considerable overhead.
- Because (locally cached) profiles are deleted after a VM reset, the logon process will typically be a little more CPU and especially IO intensive in a stateless environment.

Consequently, all desktop VM's are reset in the VMware View pool between each test in the stateless scenario's. When tests are performed in a stateful scenario, the desktop VM's are only rebooted.

8.2 DEFAULT SETTINGS

AV solutions are often tested with 'default' configuration settings. This often means all scanning features are fully enabled. This includes, scanning on both read and write (in- and outcoming), IE plug-ins, heuristic scanning and more, depending on the AV solution. However to ensure the tests show reasonable and consistent results, some settings have been changed. These are:

- **Disabled automatic updates:** this prevents virus definition files or even runtime/agent/engine being downloaded or updated during the test. If this would happen it would dramatically impact results and performance. For this

reason, it's typical to disable automatic updates in VDI environments and make sure this only happens within a designated maintenance window.

- **Disabled scheduled scans**: this has the potential for an even worse impact than automatic updates, since a scheduled scan of the system drive within one or more VMs' during a test would drain the storage subsystem from IO capacity. This would have a dramatic effect on the outcome of the test. In real world VDI environments, an accidental scheduled system scan by all VM agents will typically kill storage completely, sometimes even forcing a reset of the storage layer itself.
- **Exclude Login VSI files and exes from scan**: to prevent the AV solutions actually slowing down the test execution itself, the Login VSI executables and (log)files are excluded from real-time scanning.
- **Perform a full pre-scan of the image**, before it is deployed and cloned in the pool: to understand this one a little better, review the next section…

8.3 THE CRITICAL IMPORTANCE OF AN IMAGE PRE-SCAN

Once the VRC lab had been configured to evaluate antivirus solutions, a conventional AV product Microsoft Forefront was tested first. The outcome was surprising and much worse than originally expected.

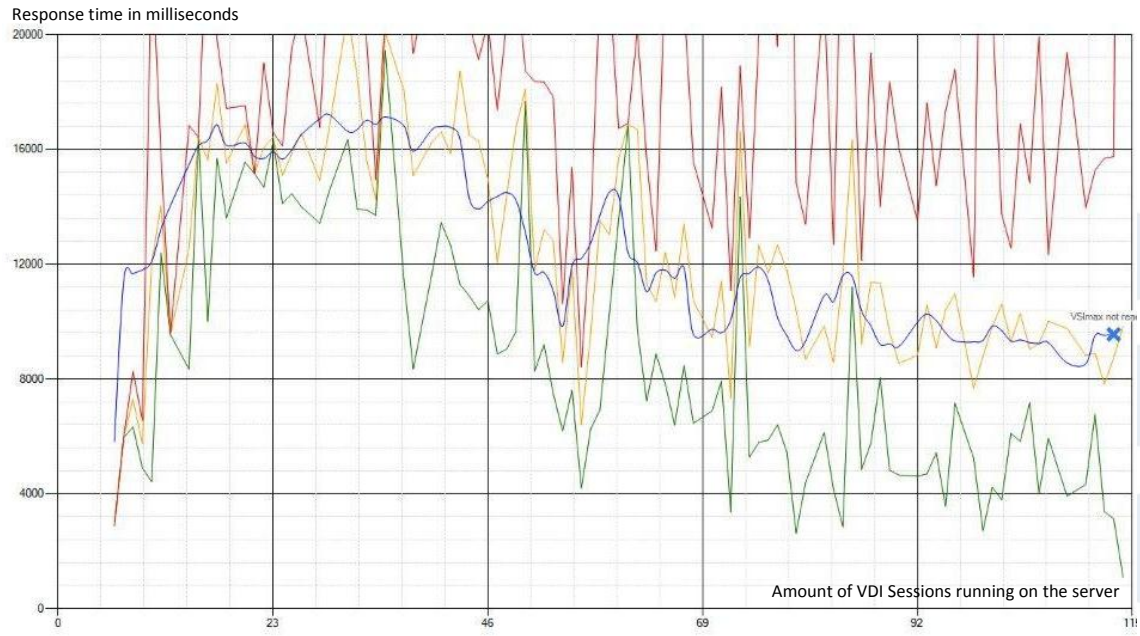


Figure 7-1 First test run results with Microsoft Forefront

The previous graph clearly shows how from the first session, Login VSI response times are going through the roof. The horizontal scale shows the amount of active users, the vertical scale represents the Login VSI response time. The green line is the minimum, the red line is the maximum, and the blue and yellow lines show averages.

The impact is quite dramatic, the response times are extremely high and are getting lower when the test continues (but remain unusually high). This is almost opposite of a normal test run, of which an example is displayed in the graph below. It is not difficult to imagine, such extreme results were quite unexpected.

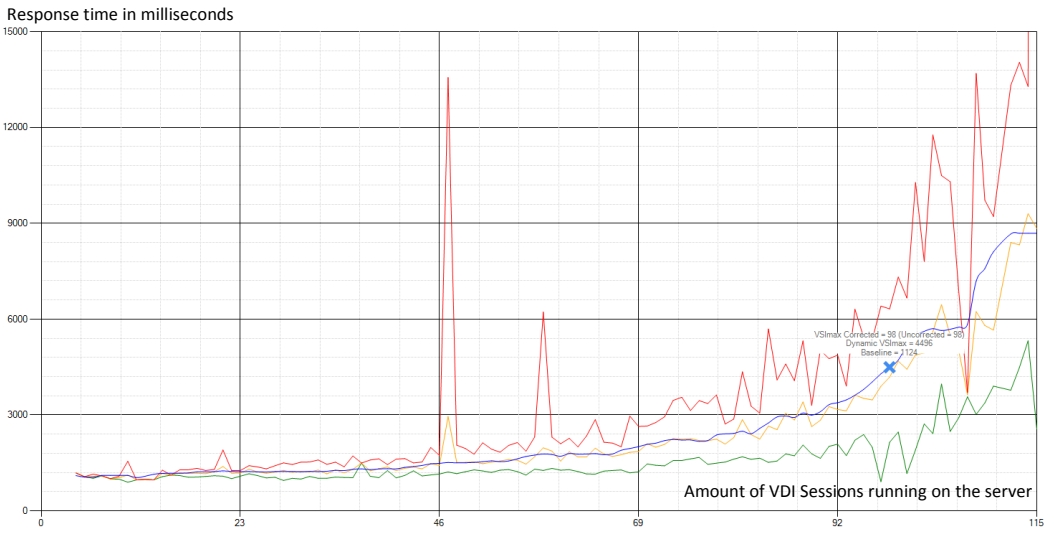


Figure 8-2 Example of a normal test run without antivirus installed

When troubleshooting was started, many options were considered: were the scheduled updates or scheduled scans running in the background (even though these were disabled through policy)? Was there a conflict or configuration mistake made? Does MS Forefront really have a tremendous impact?

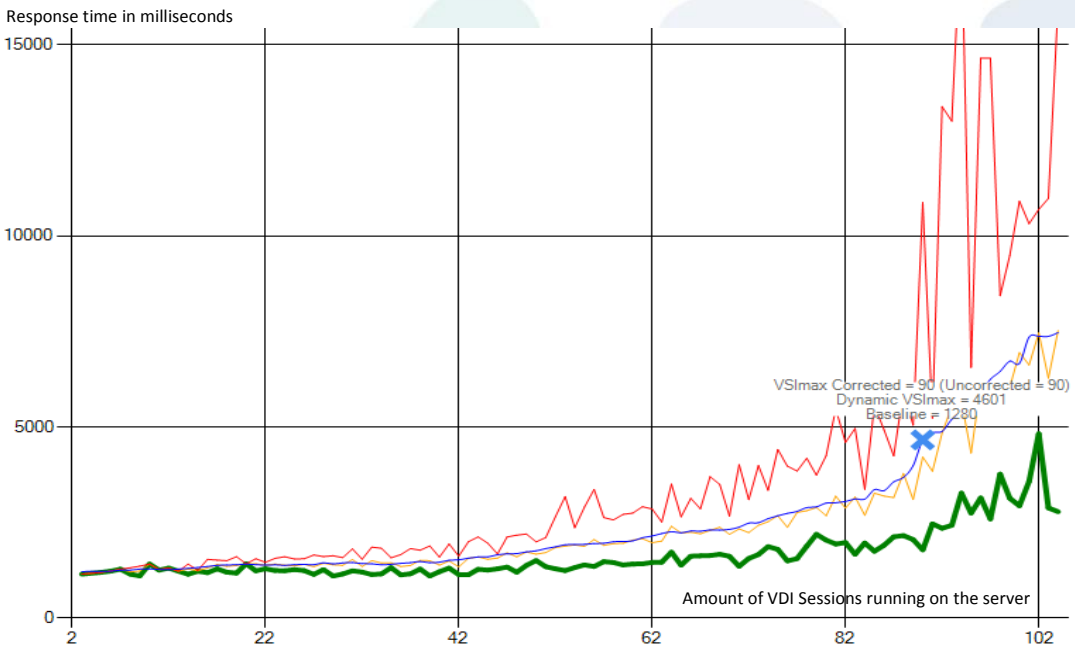


Figure 8-3 Sample of a Forefront test with a pre-scan of the master image

After testing and reviewing the configuration and policies in detail, it was decided to perform the test again. This time before a desktop pool was cloned, a full system scan was performed within the master image. The improvement was dramatic.

The explanation is simple: by performing a full pre-scan of the master image, the AV agent can create an database, hashing all files and objects scanned and flagging them as safe. The next time the same file or object is read, the antivirus agent quickly determines if the file has been previously scanned and already flagged as safe. If so, the file or object is not scanned again and skipped. Pre-scanning the image in many ways mimics the effect of disabling the scanning on 'read' option (performing only write scans).

Because the pre-scan of the image is done within the master image and before the desktop pool is created, the database of the full system scan is already available once all desktops are created in the pool. Seems quite logical right?

Project VRC has previewed these results on at the well-known seminars on desktop virtualization: BriForum, Citrix Synergy EU and US, VMworld US and others. Each time the audience was asked the same question: "Who actually does a full system scan of the golden image, before it is it's deployed?". In total more than 2000 people attended these sessions. The result was quite surprising: less than 1% raised their hand. Of course, a survey like this is not the most scientifically proven method, but getting such a low response on this question was startling. On the other hand, the authors of this document were not doing the same either, before these results were visible.

Many of the optimizations mentioned in this document are difficult to recommend. Almost all affect the scan features and reduce the security of the system. In the real world, such optimizations are a hard sell to the security officer. It's not difficult to blame him: the amount of viruses and Trojans and the sheer intelligence they deploy is steadfastly increasing.

However, Project VRC believes that 'Performing a full system scan (pre-scan) of the master image, before it's deployed' is a best practice that can be wholeheartedly recommended. It doesn't affect enterprise security guidelines and can make a dramatic improvement in performance.

Please keep in mind that the master image should not be months old before cloning a desktop pool, it could force a 'scan on read' for each file because the object database is regarded as outdated. We tested the impact of a definition update with MS Forefront. This did not have an immediate effect on the results, the agent did not regard the local database as outdated and started scanning all files and objects again. However, we cannot guarantee the same behavior can be witnessed in other AV solutions.

Because the positive performance impact of a pre-scanned image is so great, Project VRC decided to include this as a best-practice and standard for all the tests. Therefore

all tests in this document are performed with a pre-scan of the golden image before the desktops are deployed, including the default configuration scenario's.

8.4 TUNING THE ANTIVIRUS AGENT FOR PERFORMANCE

One of the key research aims of Project VRC is to evaluate performance tuning of the antivirus solutions to reduce its impact. There are a multiple ways to do this, but these vary depending on which solution is chosen. To give an example of possible performance tuning options:

- **Disable scan on read** (scanning only on 'write' or 'incoming') for real-time scanning is a typical method used to reduce the overhead of an AV agent. Because apps and documents are always read first before they are opened or started, disabling the prior scan can have considerable impact. 'Only scans on writes' is almost never configured in practice (and disable scan on read), because its performance benefit is significantly smaller, but also tends to make a system even less secure.
- **Disable heuristic scanning** is a well know performance tuning practice. The logic required to perform this is considerable, since the AV agent is actively scanning processes and threads for specific behavior in real-time to detect malware, even when it's still unknown (zero day viruses and malware). Such a feature, although not always effective, is difficult to recommend from a security perspective. However, when small performance improvements are vital, disabling heuristics can prove effective.
- **Disable IE or Outlook plug-in.** Some AV agents make it possible to disable specific plug-ins e.g. Internet Explorer or Outlook. Disabling these plug-ins can have a positive impact from a performance perspective. However it's difficult to recommend these (especially Internet Explorer and Outlook) because both the browser and the email client are probably the primary entry point for malware and viruses.
- **Disable 3rd party firewall:** Windows already has a built-in firewall, and the phase III publication of Project VRC proves that the firewall almost has no impact on performance or desktop capacity. While the 3rd party firewall potentially has more and better security features it may be beneficial to disable the 3rd party firewall and leave the original Windows firewall enabled.

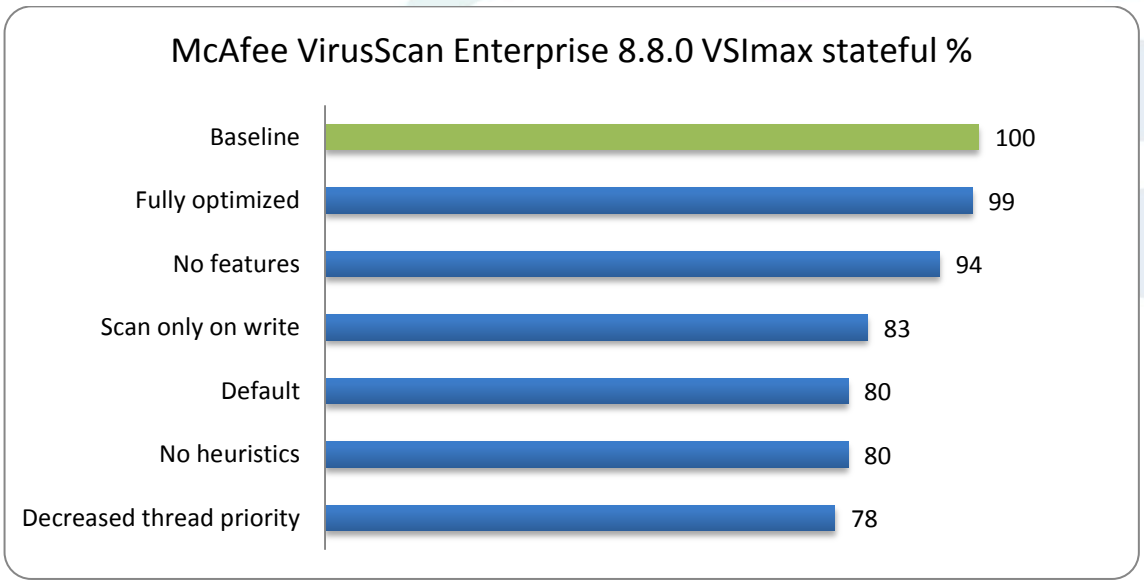
9. MCAFEE VIRUSSCAN ENTERPRISE 8.8.0

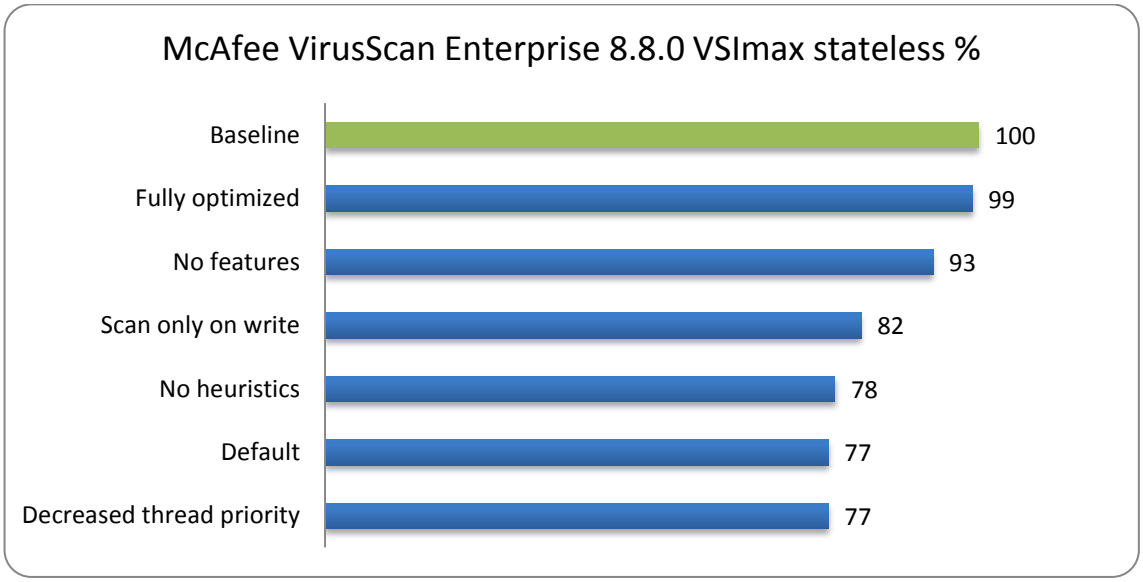
McAfee End Point Protection is one of the most widely used AV solutions in the enterprise today. 24% of the 1000 participants Project VRC 'State of the VDI and SBC Union' survey stated they were using McAfee End Point Protection within their organization.

9.1 VSIMAX RESULTS

Reviewing the VSImax results in comparison to the baseline results without AV in percentages (higher is better), the following observations are possible:

- Even when the image is pre-scanned, configuring to 'scan only on write' does lower the impact of AV.
- Fully optimized the overhead is minimal, but this should be considered a very unsafe configuration
- Looking at the 'no features' results, it is clear that disabling self-healing and buffer overflow protection saves a lot of resources. However, from a security point of view these are difficult to recommend.
- Disabling heuristics has a much smaller effect than expected. Heuristics has a reputation of generating a lot of overhead, but in this test this does not seem the case. We can only speculate why: this trend is consistent throughout all tests performed with only heuristics disabled.
- The difference between stateless and stateful is very small, however, the impact is a little lower for stateful in comparison to stateless, this is expected.

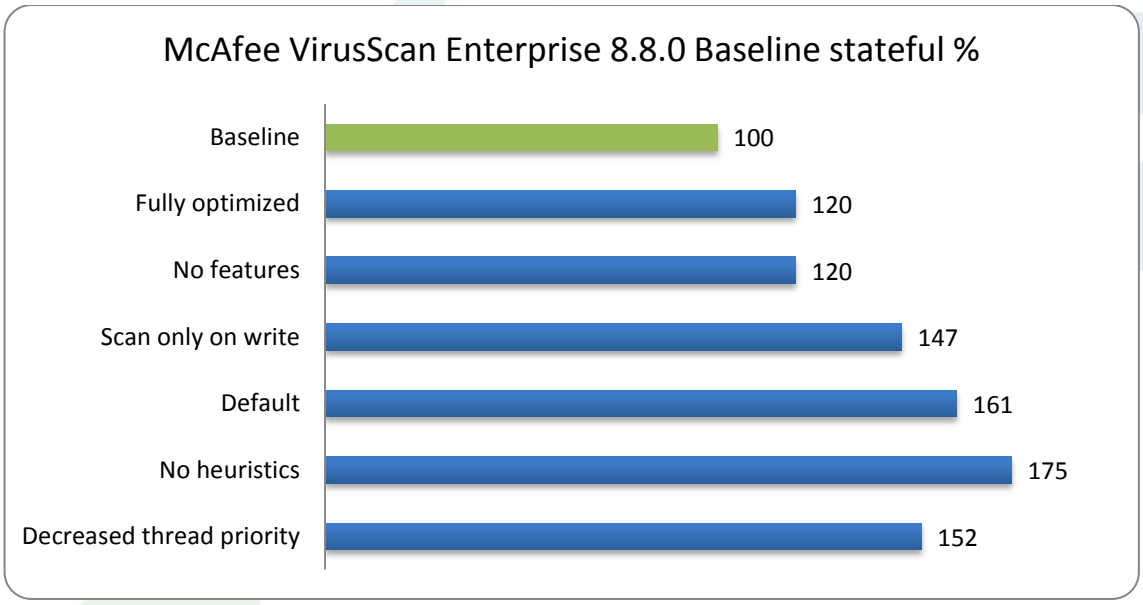


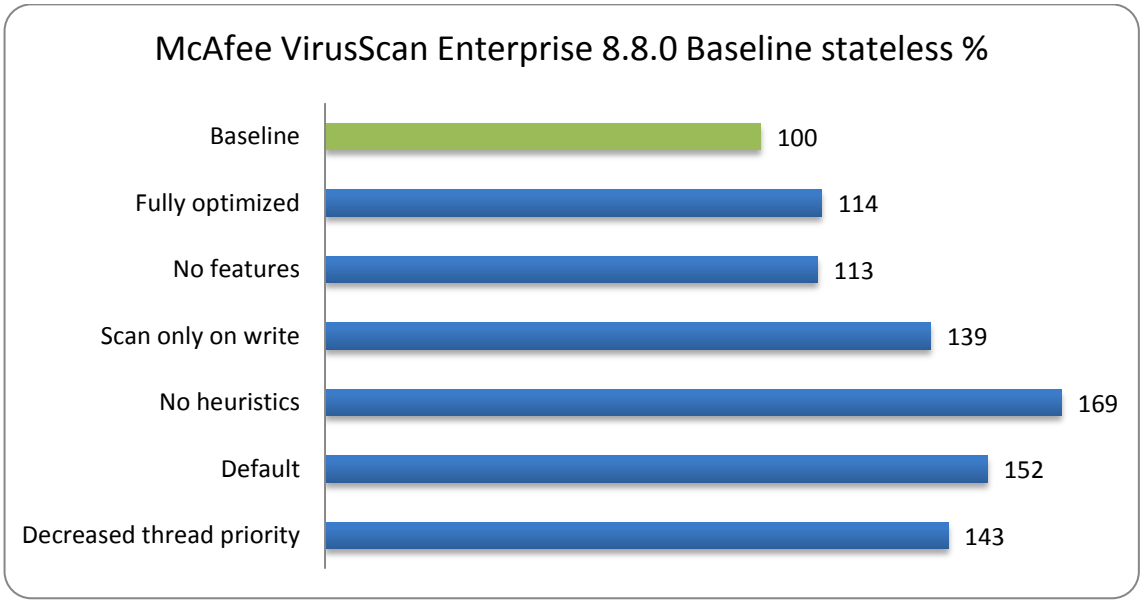


9.2 BASELINE LOGIN VSI RESPONSE TIME RESULTS

Reviewing baseline response time for the VSImax results in comparison to the baseline results without AV in percentages (lower is better), the following observations are possible:

- When fully optimized, the AV overhead is only 13% for stateless VDI, while it is 20% in stateful VDI.
- Interestingly, looking at the 'No Heuristics' tests, where only heuristics are disabled, the response time increases in comparison to the default. This trend is also visible in disk IO results. Since this behavior is not logically to explain, it is probably the result of a bug. Disabling heuristic scanning should lower the AV overhead, not increase it.

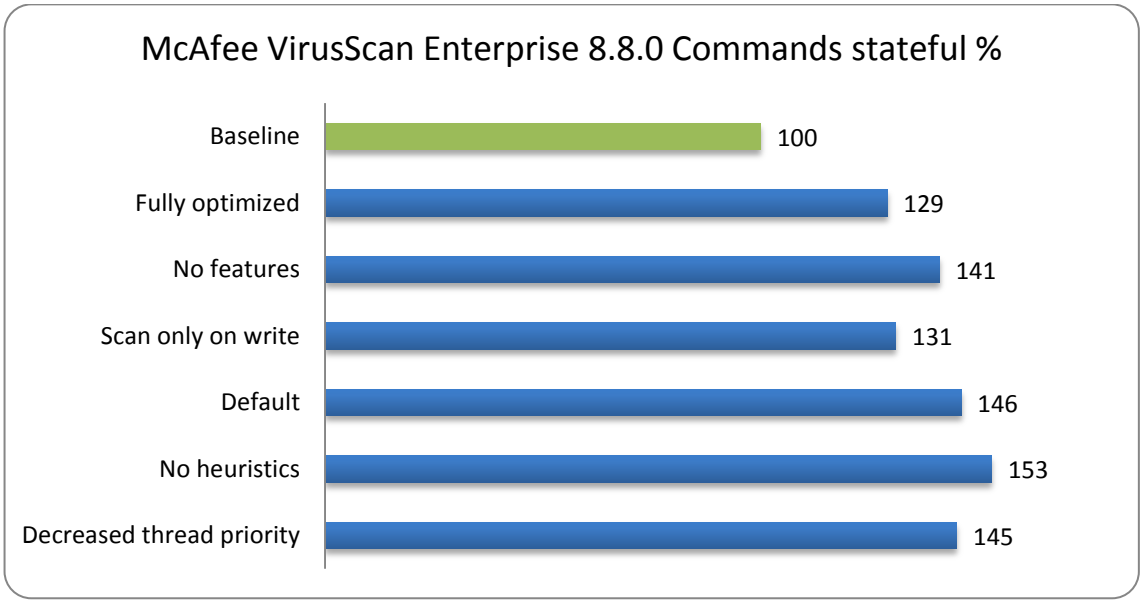


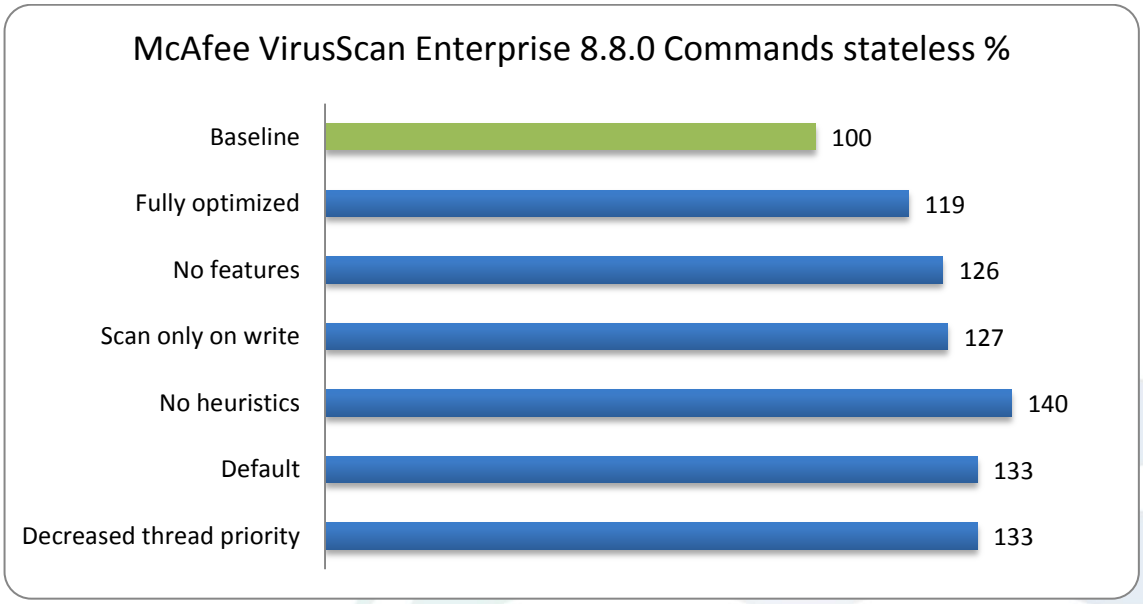


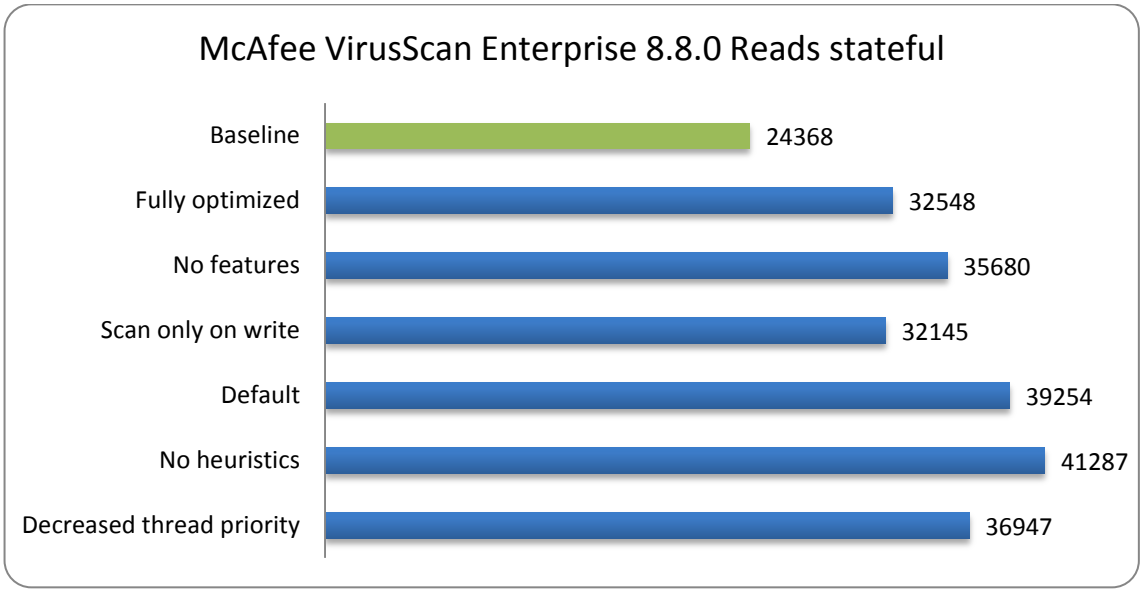
9.3 DISK IO RESULTS

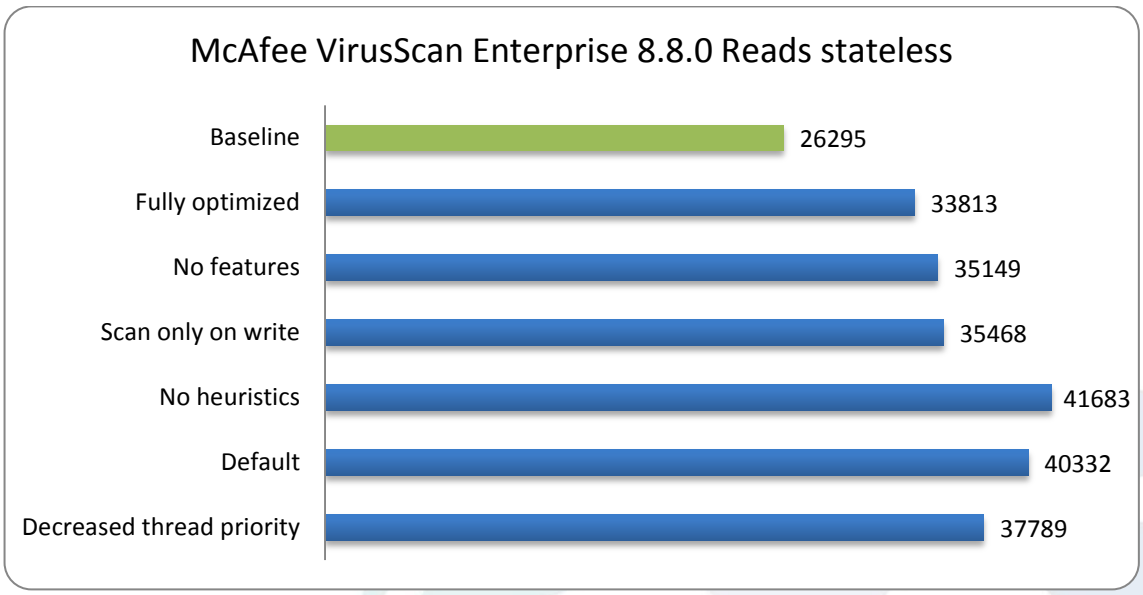
Reviewing disk IO total command (including total reads and writes) results, when 50 Login VSI sessions are logged on (lower is better), the following observations are possible:

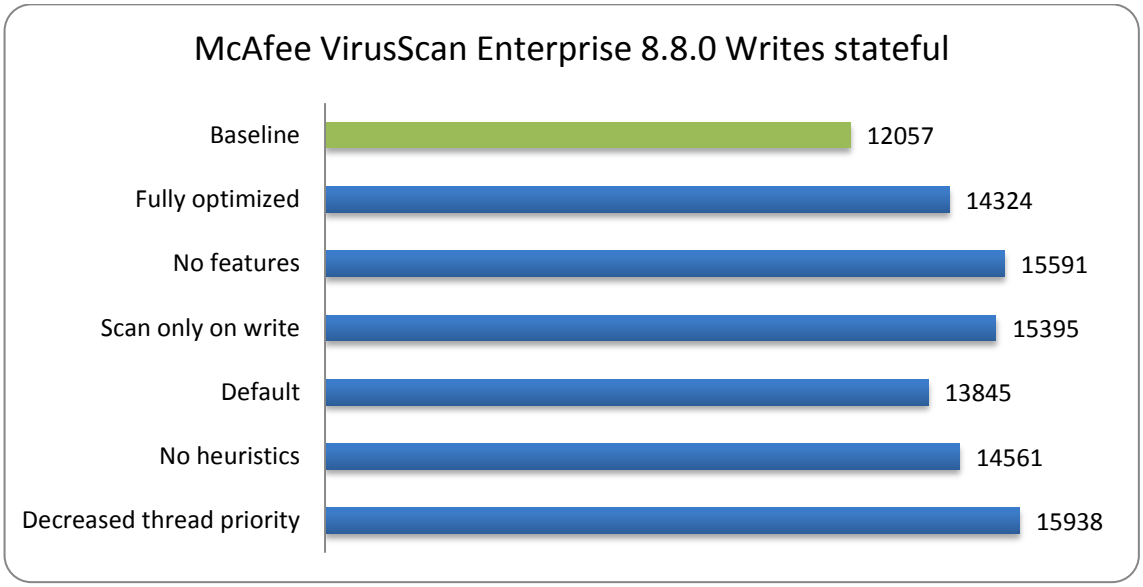
- The highest IO overhead measured in total is around 50%
- Optimizations lower IO impact down to 29% in stateful and to 19% in stateless environments.
- Overall, the IO results do show higher than typical randomness between configurations, for this no specific explanation has been found.
- Overall, the IO footprint overhead is not very high, especially compared to other solutions. However, we did not test without a pre-scan of the master image: this could potentially show completely different results.

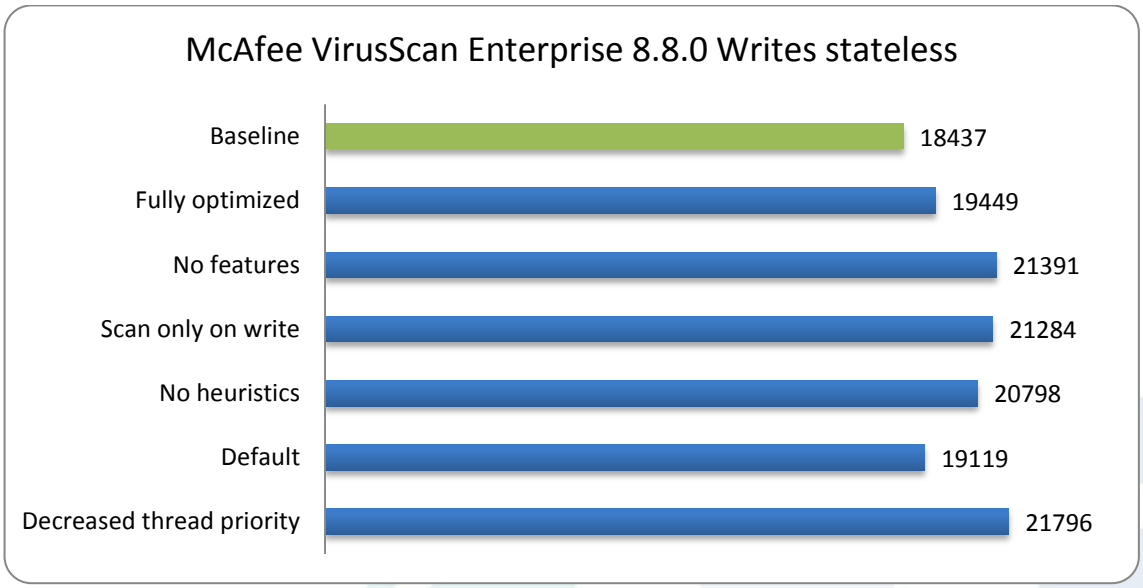

McAfee VirusScan Enterprise 8.8.0 Commands stateful %
Baseline
100
Fully optimized
129
No features
141
Scan only on write
131
Default
146
No heuristics
153
Decreased thread priority
145


McAfee VirusScan Enterprise 8.8.0 Commands stateless %
Baseline
100
Fully optimized
119
No features
126
Scan only on write
127
No heuristics
140
Default
133
Decreased thread priority
133


McAfee VirusScan Enterprise 8.8.0 Reads stateful
Baseline
24368
Fully optimized
32548
No features
35680
Scan only on write
32145
Default
39254
No heuristics
41287
Decreased thread priority
36947


McAfee VirusScan Enterprise 8.8.0 Reads stateless
Baseline
26295
Fully optimized
33813
No features
35149
Scan only on write
35468
No heuristics
41683
Default
40332
Decreased thread priority
37789

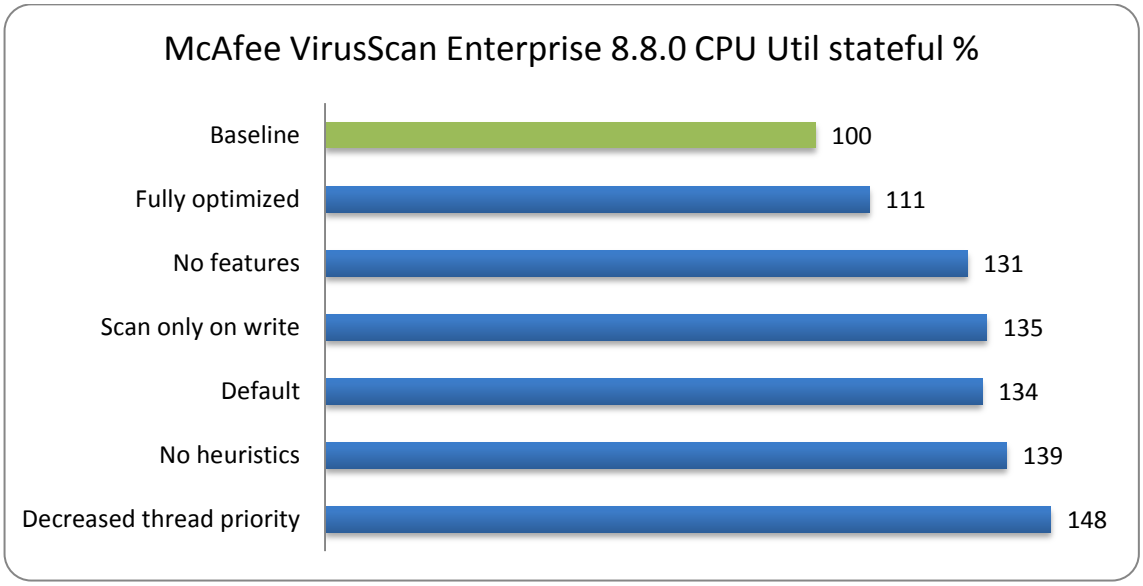


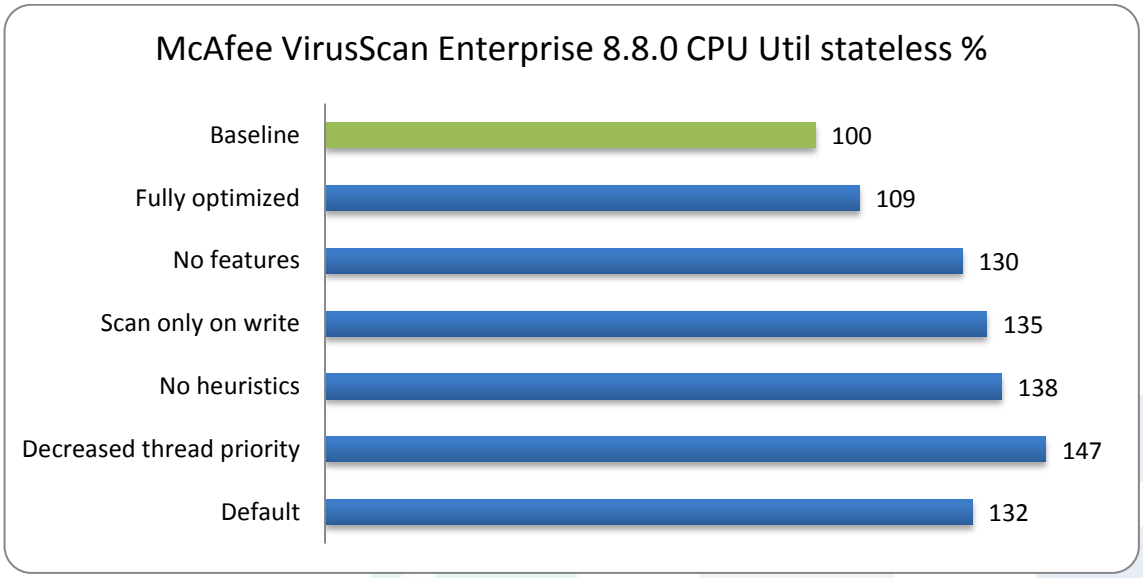


9.4 CPU UTILIZATION WITH 50 SESSIONS

Reviewing the average total Processor Utilization in percentages, when 50 Login VSI sessions are logged on (lower is better), the following observations are possible:

- Fully optimized, the CPU overhead is minimized to 10%
- Worst CPU overhead is witnessed when the Decrease thread priority option is set: to around 50%


McAfee VirusScan Enterprise 8.8.0 CPU Util stateful %
Baseline
100
Fully optimized
111
No features
131
Scan only on write
135
Default
134
No heuristics
139
Decreased thread priority
148


McAfee VirusScan Enterprise 8.8.0 CPU Util stateless %
Baseline
100
Fully optimized
109
No features
130
Scan only on write
135
No heuristics
138
Decreased thread priority
147
Default
132

9.5 OVERVIEW OF SETTINGS

Default		
Configuration	***Setting***	***Description***
Disable auto update after client install (initial update needed)		
on-access scan\all processes\exclusions (including subfolders for all)	B:\	
	G:\	
	H:\	
	C:\Program Files\Login Consultants\VSI\	
No features		
This configuration is the same as Default except for some features installed during installation		
ONLY install the following features:		
autoupdate (initial update)		
Scan on access		
Scan on demand (for pre-scan)		
Decreased thread priority		
This configuration is the same as Default except for the following registry key		
Disable self protection		
Add reg key HKLM\SOFTWARE\Network Associates\TVD\Shared Components\Framework	LowerWorkingThreadPriority : 1	
restart McAfee Framework Service:		
enable self protection		
Scan only on write		
This configuration is the same as MA NoOpt except for the following registry key		
Configuration	***Setting***	***Description***
on-access scan\all processes\scan items	Disable scan files when reading from disk	Only scan on write
	Disable scan files opened for backup	Only scan on write
MA Opt		
MA Opt is a combination of Default, No features, Decreased thread priority, Scan only on write and No heuristics		
Configuration	***Setting***	***Description***
Disable autoupdate after client install (initial update needed)		
on-access scan\all processes\exclusions (including subfolders for all)	B:\	
	G:\	
	H:\	
	C:\Program Files\Login Consultants\VSI\	
on-access scan\all processes\scan items	Disable scan files when reading from disk	Only scan on write
	Disable scan files opened for backup	Only scan on write

Disable self protection		
Add reg key HKLM\SOFTWARE\Network Associates\TVD\Shared Components\Framework	LowerWorkingThreadPriority : 1	
restart McAfee Framework Service:		
enable self-protection		
ONLY install the following features:		
auto update (initial update)		
Scan on access		
Scan on demand (for pre-scan)		

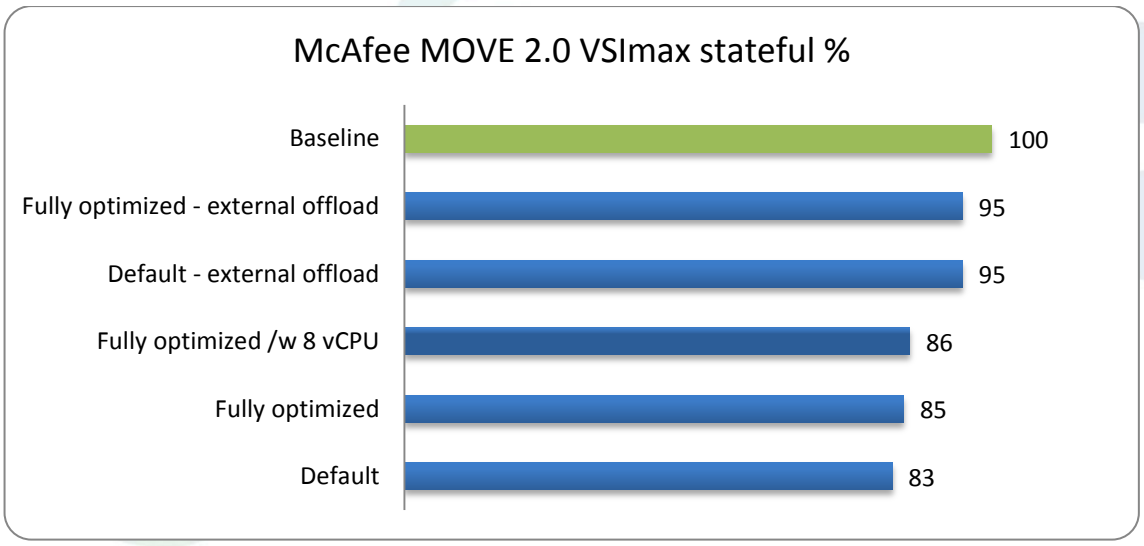
10. MCAFEE MOVE MULTIPLATFORM 2.0

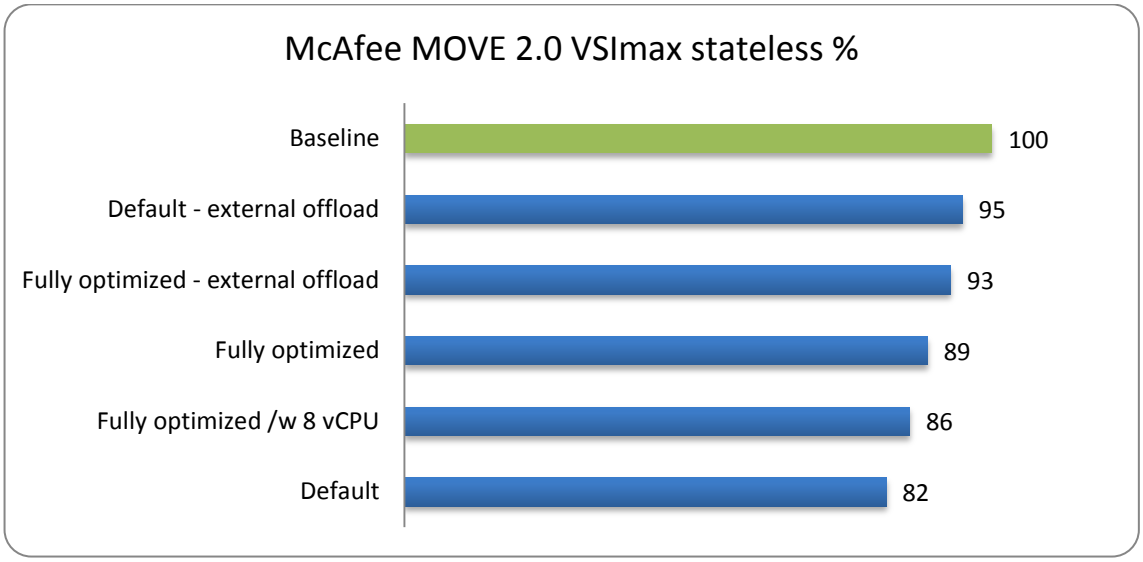
McAfee MOVE Multiplatform 2.0 offloads AV scanning through the network to a Windows 2008 Server with a Antivirus scanning service. McAfee MOVE multiplatform can be run on any hypervisor and the off-loading VM can run on a different host than the Desktop VM's. 2% of the Project VRC Survey participants mentioned they were using McAfee MOVE.

10.1 VSIMAX RESULTS

Reviewing the VSImax results in comparison to the baseline results without AV in percentages (higher is better), the following observations are possible:

- The difference between stateful and stateless desktop VM's is very small.
- Optimizations have minimal performance benefit
- Adding additional vCPU's to the offloading VM does not significantly increase performance.
- In the default configuration, the overhead is around 18%
- Logically, when the offloading VM is running on a different host the total overhead is further reduced to 5%. However, this configuration is not completely fair to other solutions, since additional physical resources are used on a separate host. This option is only possible with McAfee MOVE Multiplatform
- From a VSImax perspective, the default configuration clearly performs better than the conventional McAfee AV solution.

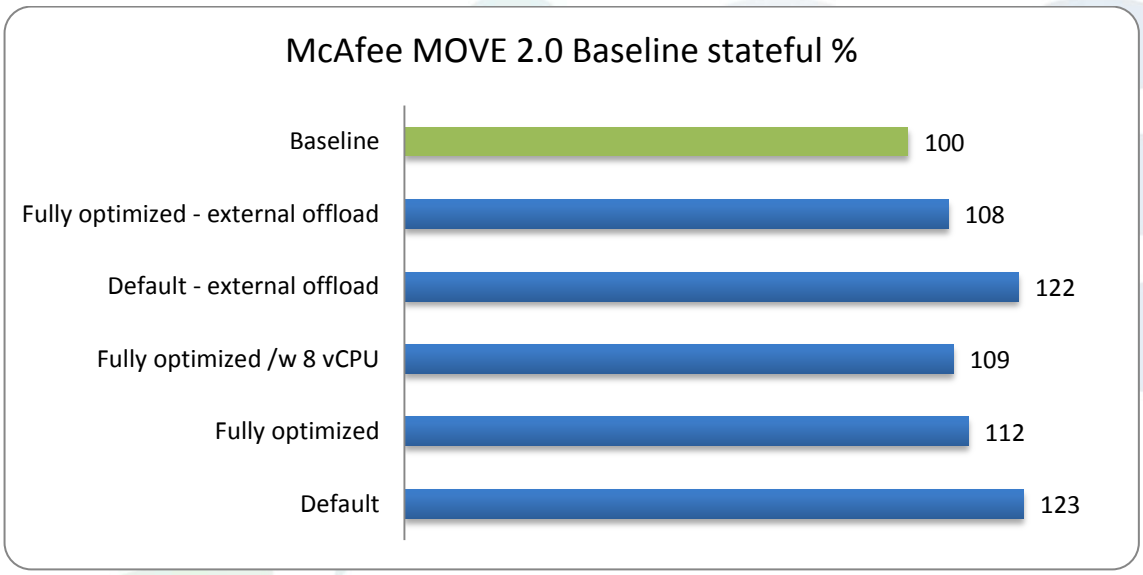


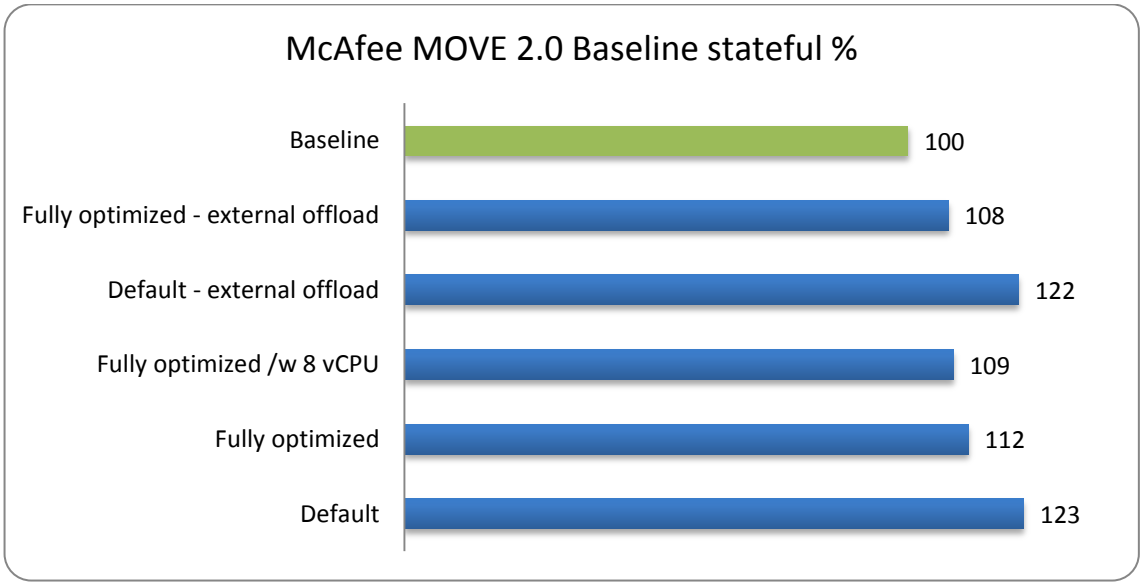


10.2 BASELINE LOGIN VSI RESPONSE TIME RESULTS

Reviewing baseline response time for the VSImax results in comparison to the baseline results without AV in percentages (lower is better), the following observations are possible:

- The highest overhead on the Login VSI response time is 23%.
- Optimizing reduces overhead to around 9%
- Configuring the offloading VM to run on a different server does not change the response time overhead significantly

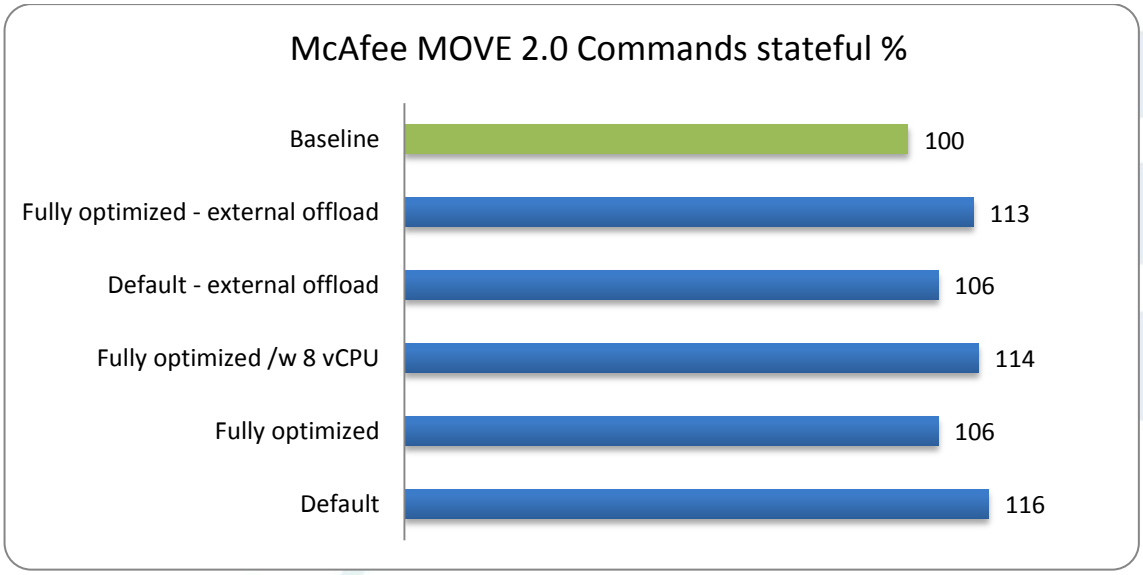


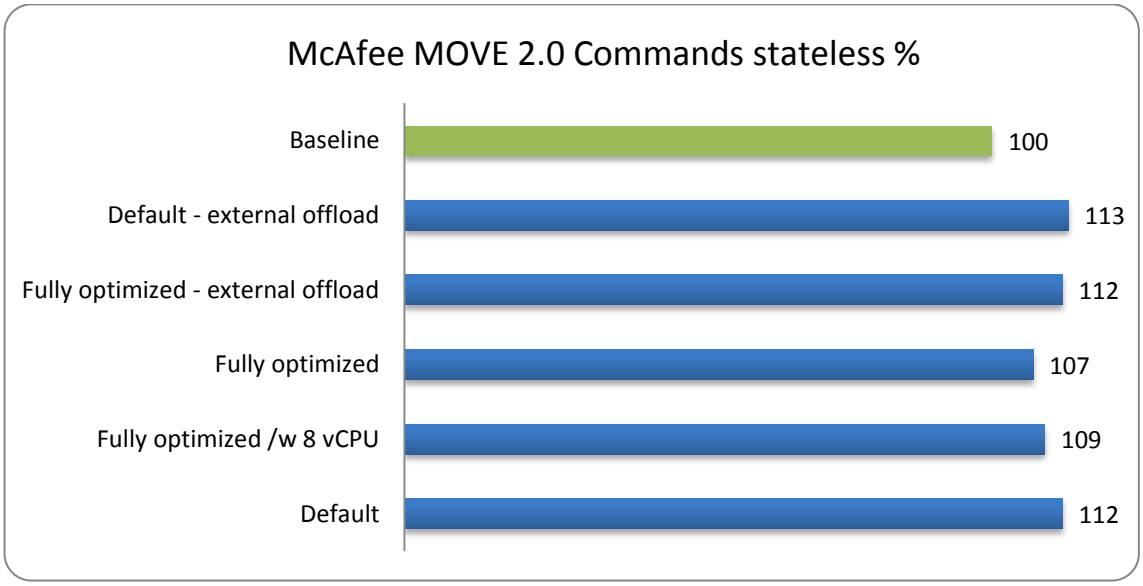


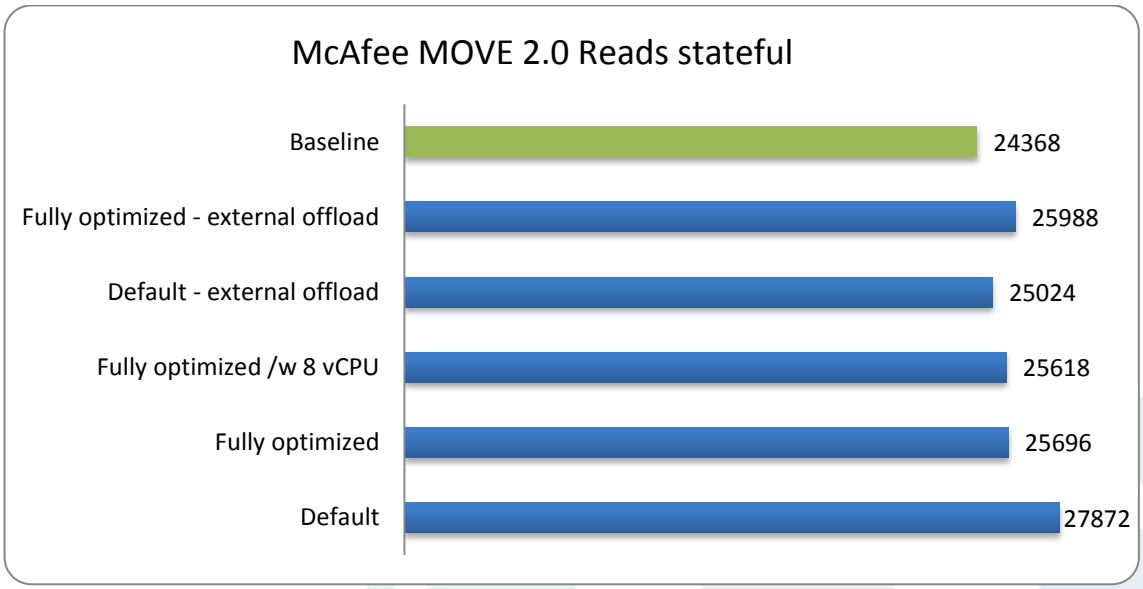
10.3 DISK IO RESULTS

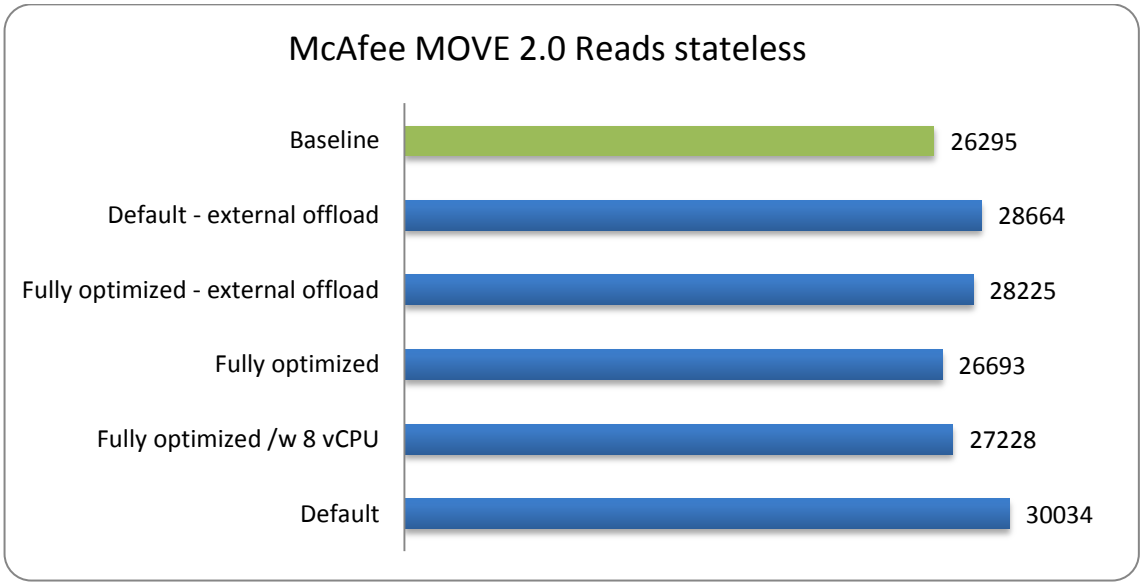
Reviewing disk IO total command (including total reads and writes) results, when 50 Login VSI sessions are logged on (lower is better), the following observations are possible:

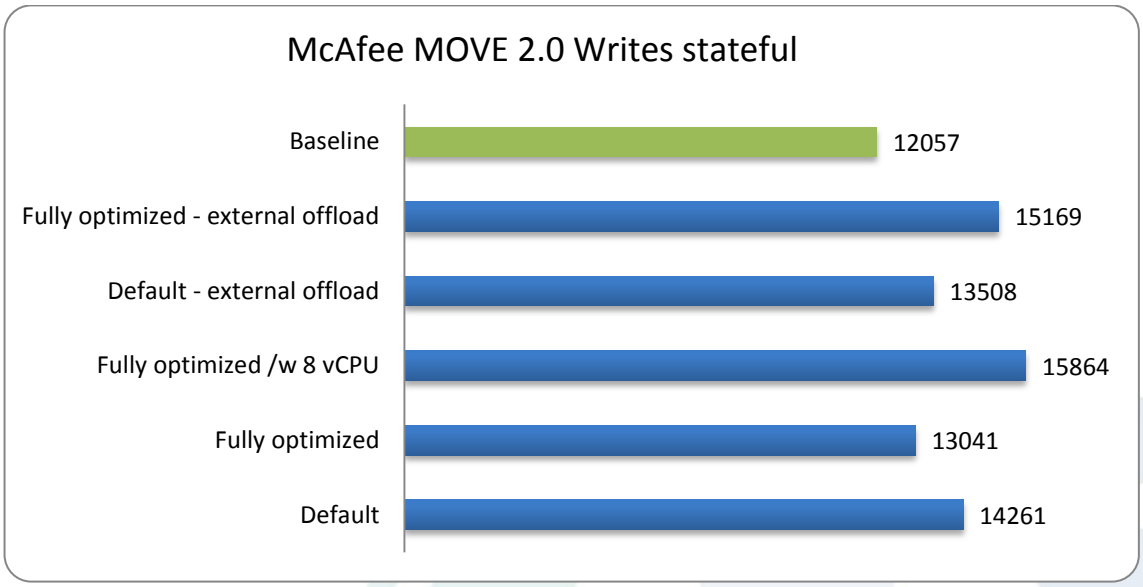
- The highest total IO overhead measured is 16%
- Overall, the disk IO overhead is small in comparison to conventional AV solutions: here the offloading architecture clearly proves itself.

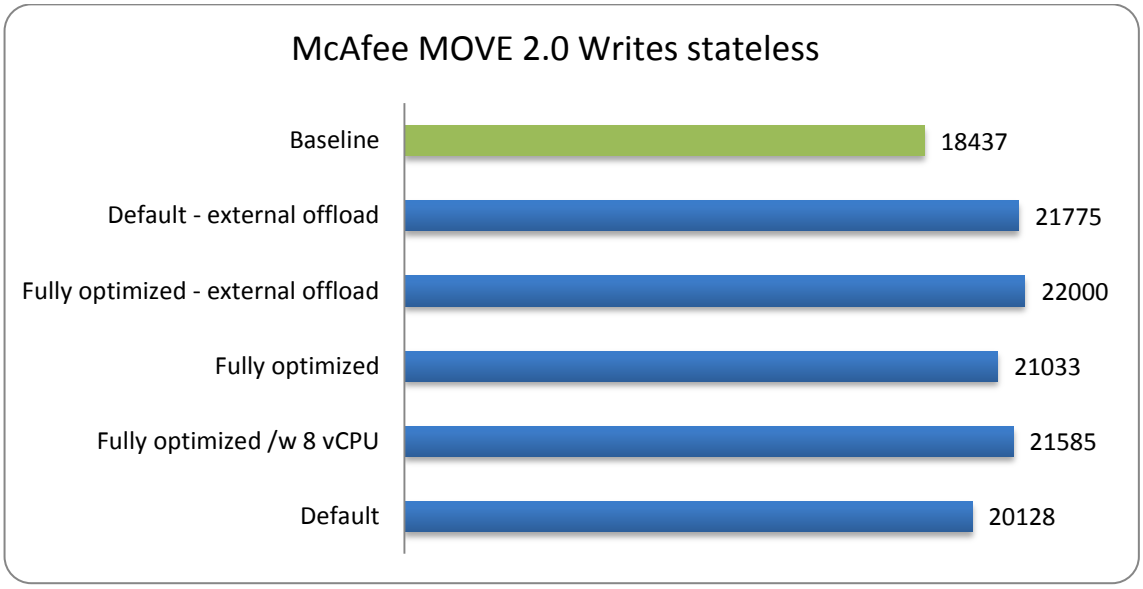



McAfee MOVE 2.0 Commands stateless %
Baseline
100
Default - external offload
113
Fully optimized - external offload
112
Fully optimized
107
Fully optimized /w 8 vCPU
109
Default
112


McAfee MOVE 2.0 Reads stateful
Baseline
24368
Fully optimized - external offload
25988
Default - external offload
25024
Fully optimized /w 8 vCPU
25618
Fully optimized
25696
Default
27872


McAfee MOVE 2.0 Reads stateless
Baseline
26295
Default - external offload
28664
Fully optimized - external offload
28225
Fully optimized
26693
Fully optimized /w 8 vCPU
27228
Default
30034

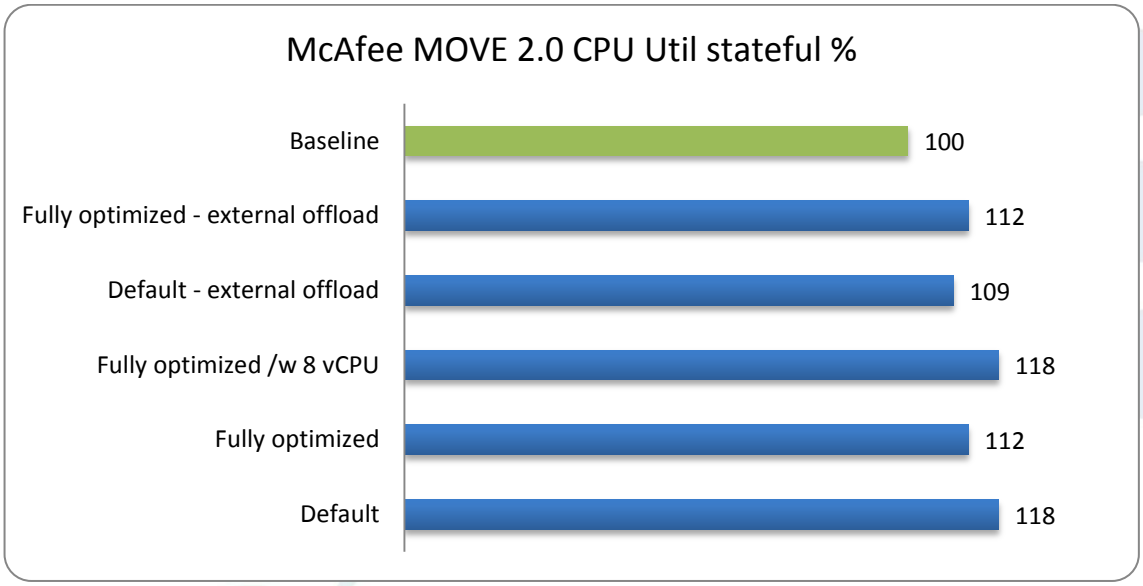

McAfee MOVE 2.0 Writes stateful
Baseline
12057
Fully optimized - external offload
15169
Default - external offload
13508
Fully optimized /w 8 vCPU
15864
Fully optimized
13041
Default
14261

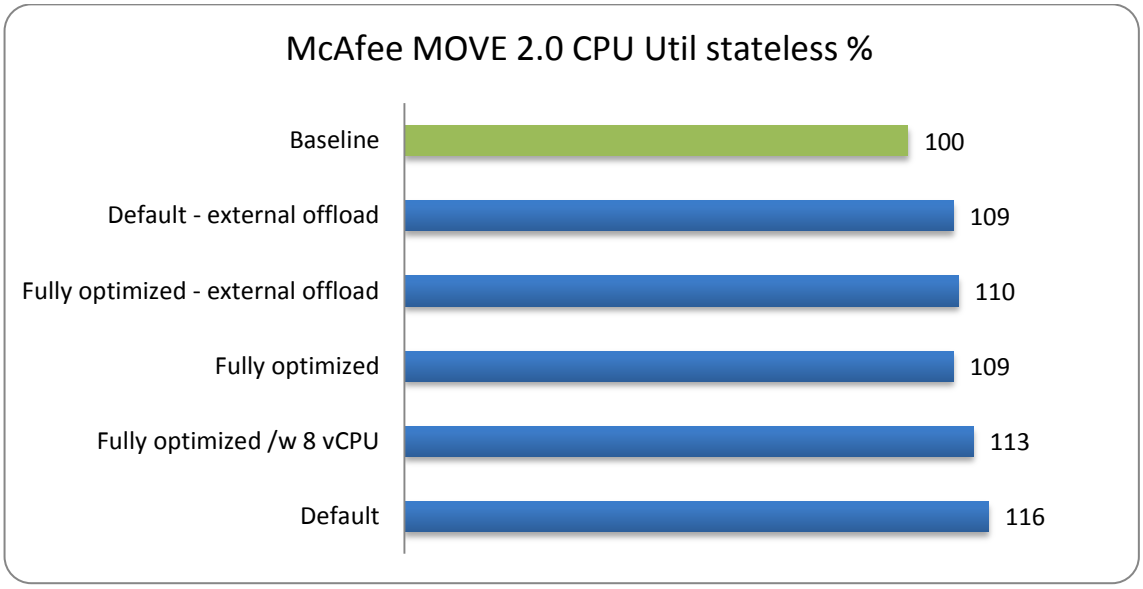


10.4 CPU UTILIZATION WITH 50 SESSIONS

Reviewing the average total Processor Utilization, when 50 Login VSI sessions are logged on (lower is better), the following observations are possible:

- At 50 sessions, the maximum CPU overhead is measured around 17%. This is significantly better than the conventional McAfee solution.
- When the offloading VM is located on a different host, it is only logical that the total processor time utilization is around 10% lower.





10.5 OVERVIEW OF SETTINGS

Default		
Configuration	***Setting***	***Description***
During offload server setup/Disable auto updates		
During server setup/Global Threat Intelligence	very low (default)	heuristics
Disable autoupdate		Disables (definition) updates
Path exclusions:	C:\Program files\Login Consultants\VSI	
	B:\	
	G:\	
	H:\	
Remove agent GUID	https://kc.mcafee.com/corporate/index?page=content&id=KB56086	
Fully Optimized		
Configuration	***Setting***	***Description***
During server setup/Global Threat Intelligence	Disabled	Disable heuristics
Path exclusions:	C:\Program files\Login Consultants\VSI	
	B:\	
	G:\	
	H:\	
Disable scan files when:	when reading from disk	Only scan files when written to
	opened for backup	Only scan files when written to
Remove agent GUID	https://kc.mcafee.com/corporate/index?page=content&id=KB56086	

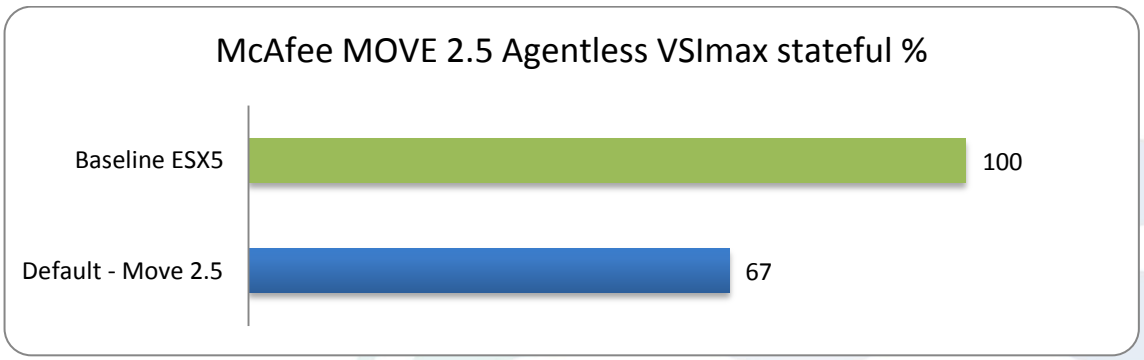
11. MCAFEE MOVE AGENTLESS 2.5

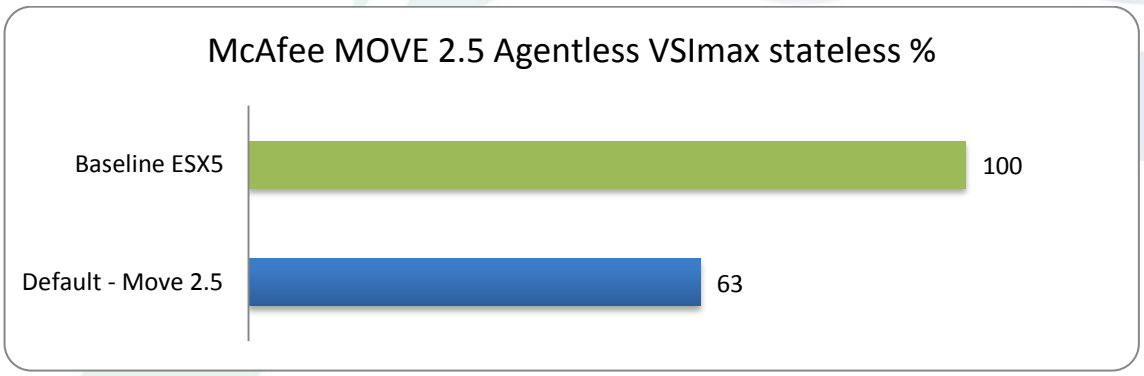
McAfee MOVE Agentless 2.5 uses a different offloading architecture than McAfee MOVE 2.0 Multiplatform. McAfee MOVE 2.5 uses the vShield driver architecture from VMware and is therefore specific to vSphere. Normally all AV tests were executed on vSphere 4.1 hosts, however, for this McAfee MOVE 2.5 to function, vSphere 5.0 was used. 2% of the Project VRC Survey participants mentioned they were using McAfee MOVE, but these are also MOVE Multiplatform deployments.

11.1 VSIMAX RESULTS

Reviewing the VSImax results in comparison to the baseline results without AV in percentages (higher is better), the following observations are possible:

- The difference between stateful and stateless desktop VM's is small, however, the impact is lower for stateful in comparison to stateless.
- From a VSImax perspective, McAfee MOVE Agentless has a considerable impact. Up to 33 % for stateful, up to 37% for stateless.
- It must be noted that the complete server is rebooted between each test: as a result the offload VM will also reset its database of scanned files and objects.

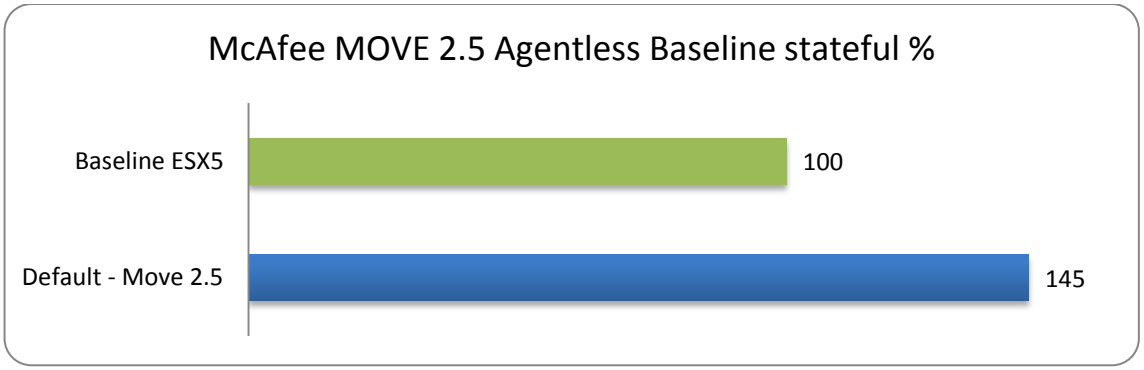


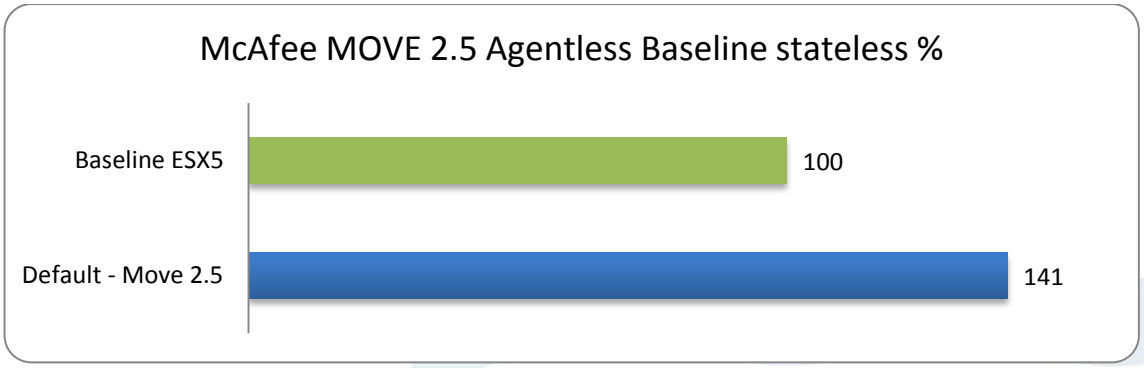


11.2 BASELINE LOGIN VSI RESPONSE TIME RESULTS

Reviewing baseline response time for the VSImax results in comparison to the baseline results without AV in percentages (lower is better), the following observations are possible:

- It is clear that the offloading architecture does affect the baseline response time of the Login VSI measurements. For both the stateful and stateless test it was above 40%.

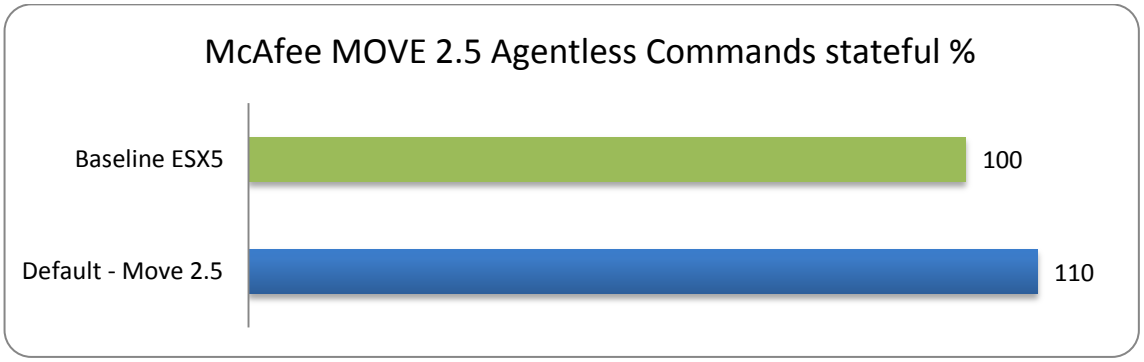


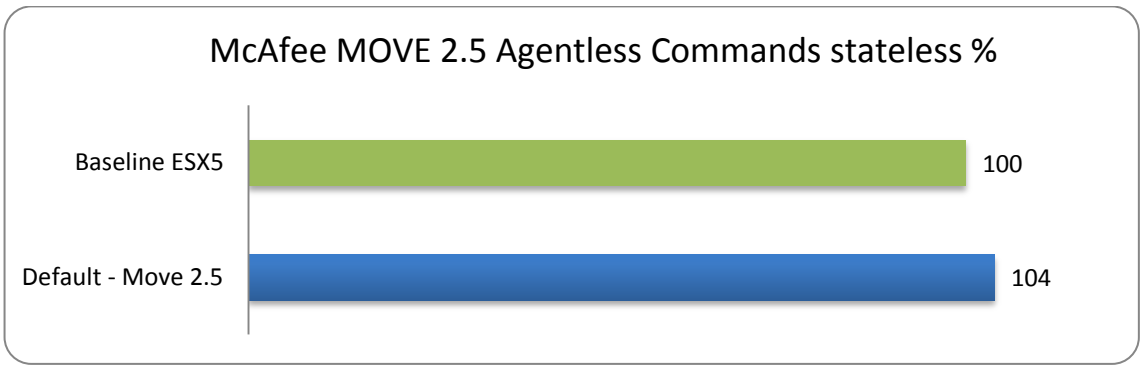


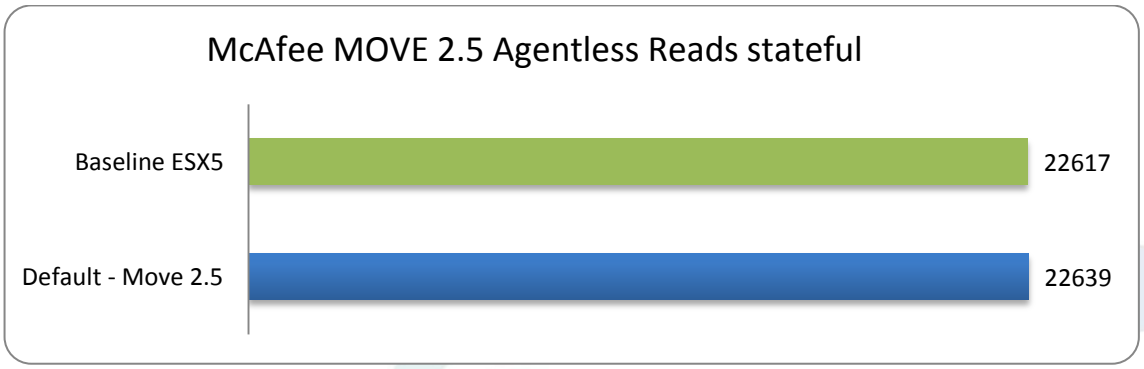
11.3 DISK IO RESULTS

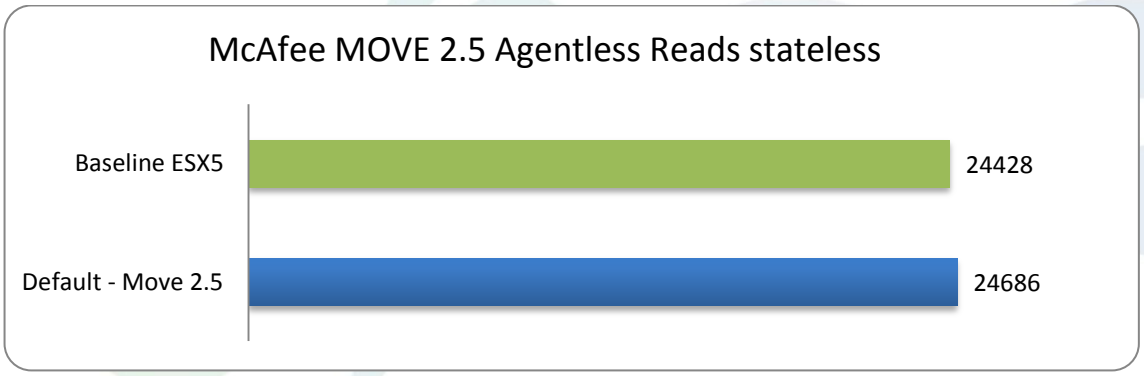
Reviewing disk IO total command (including total reads and writes) results, when 50 Login VSI sessions are logged on (lower is better), the following observations are possible:

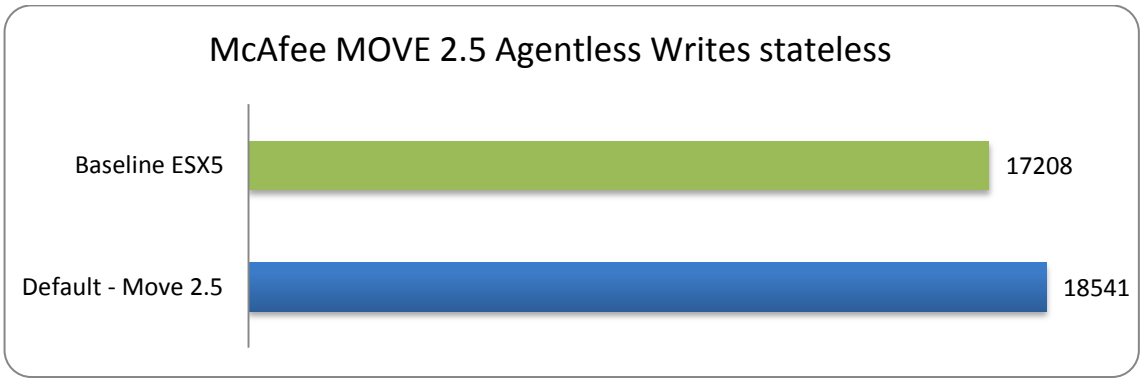
- The total IO overhead is no more than 10%.
- In contrast to most AV solutions, there is more overhead from a write perspective in comparison to read IO. However, this difference is not significant, especially compared to other solutions.
- There is no read overhead when McAfee MOVE 2.5 agentless is used.


McAfee MOVE 2.5 Agentless Commands stateful %
Baseline ESX5
100
Default - Move 2.5
110


McAfee MOVE 2.5 Agentless Commands stateless %
Baseline ESX5
100
Default - Move 2.5
104


McAfee MOVE 2.5 Agentless Reads stateful
Baseline ESX5
22617
Default - Move 2.5
22639

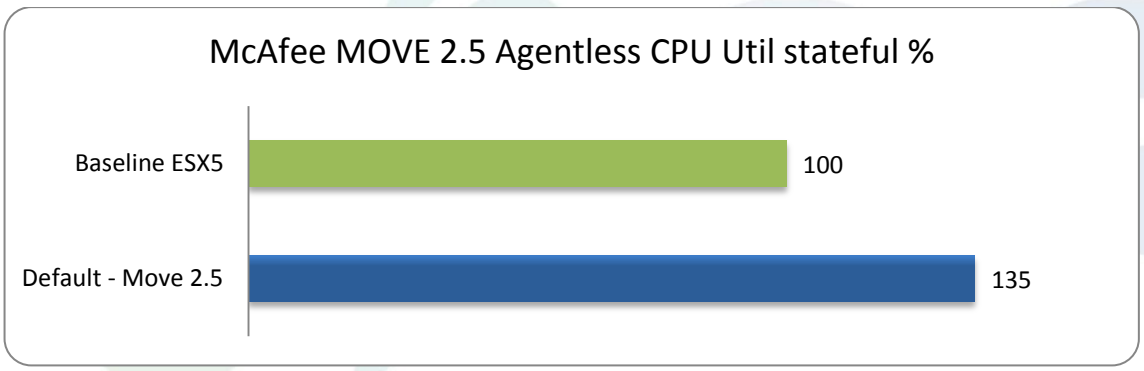

McAfee MOVE 2.5 Agentless Reads stateless
Baseline ESX5
24428
Default - Move 2.5
24686

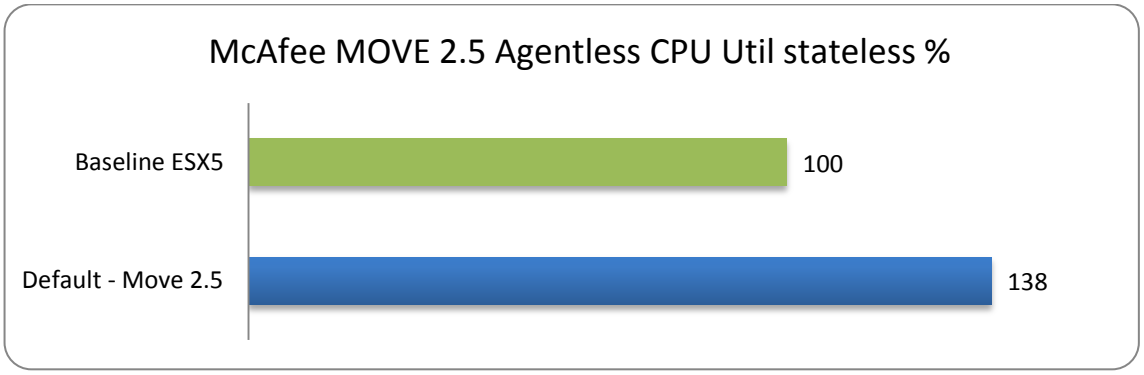


11.4 CPU UTILIZATION WITH 50 SESSIONS

Reviewing the average total Processor Utilization, when 50 Login VSI sessions are logged on (lower is better), the following observations are possible:

- Similar to VSImax, average CPU utilization was up almost 35%. It does seem this architecture is more efficient from a disk IO perspective, but not from a CPU point of view.





11.5 OVERVIEW OF SETTINGS

Note: McAfee MOVE 2.5 was only tested with default settings.

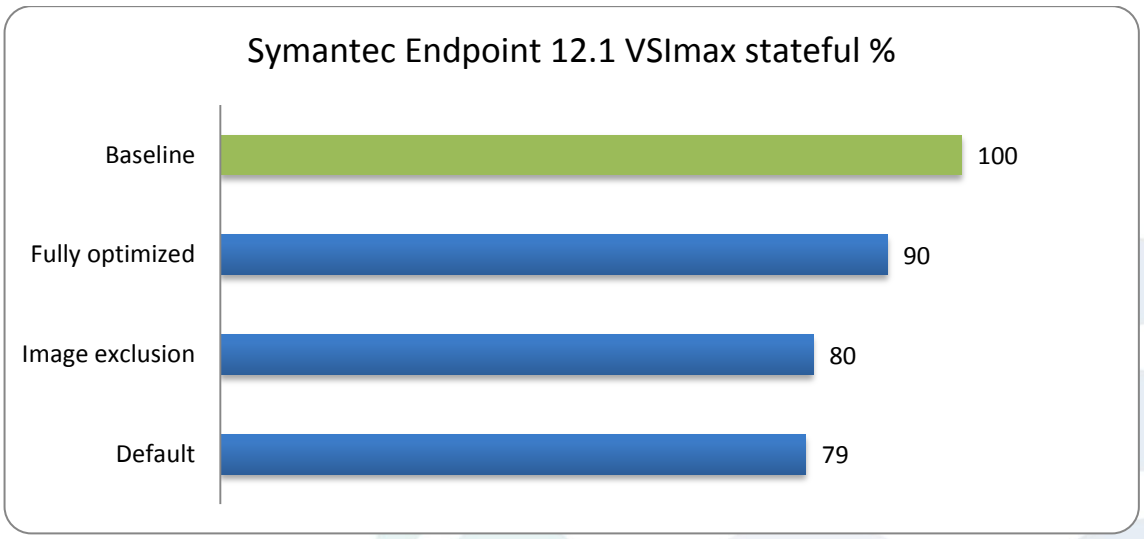
12. SYMANTEC ENDPOINT PROTECTION 12.1

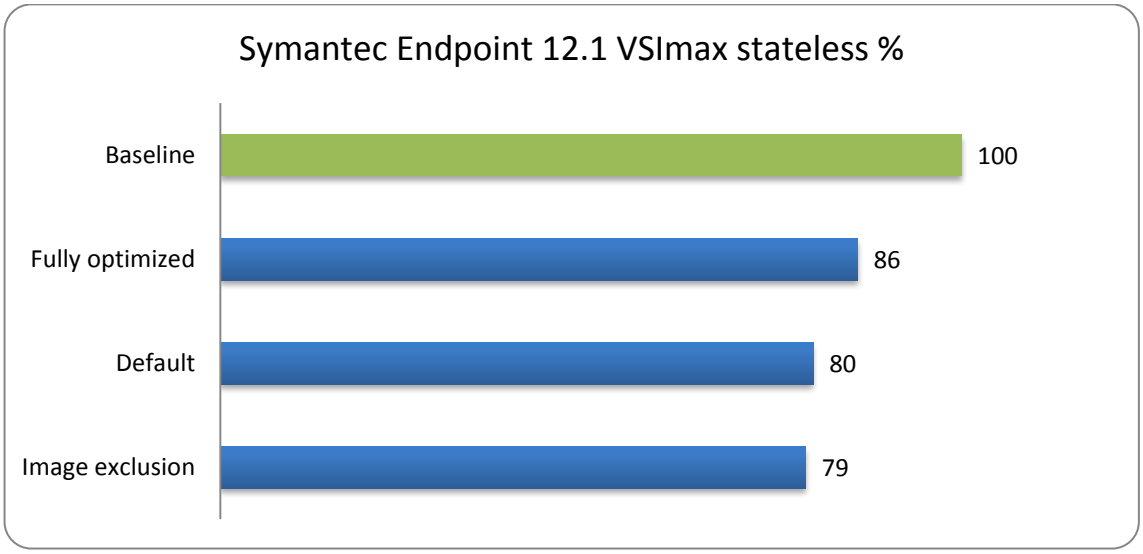
After McAfee, Symantec is the second most popular conventional AV solution, 20% of the Project VRC participants indicated they were using Symantec.

12.1 VSIMAX RESULTS

Reviewing the VSImax results in comparison to the baseline results without AV in percentages (higher is better), the following observations are possible:

- Both in stateful and stateless configuration, Symantec's performance impact is about 21%.
- Because the image is already pre-scanned, configuring image exclusion option does not have a significant impact.
- The difference in impact between stateful and stateless desktop VM's is very small.
- Fully optimized the impact ranges from 10% (stateful) to 14% (stateless).

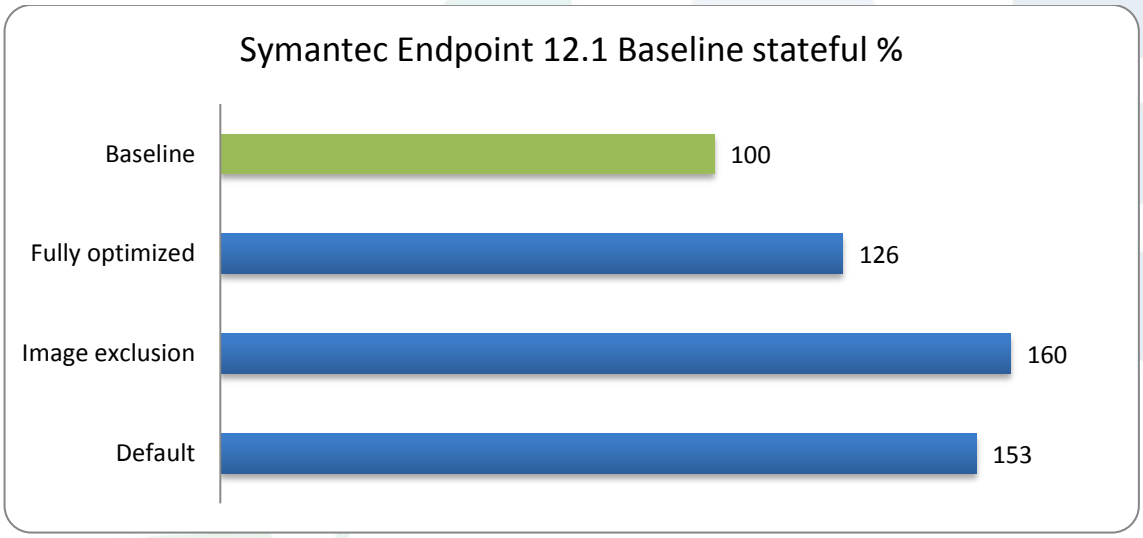


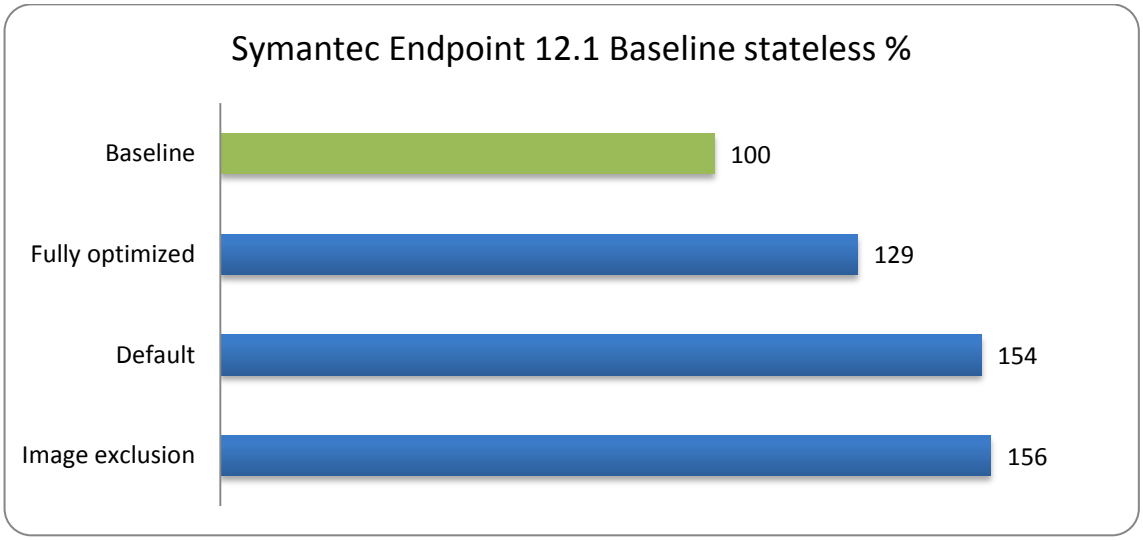


12.2 BASELINE LOGIN VSI RESPONSE TIME RESULTS

Reviewing baseline response time for the VSImax results in comparison to the baseline results without AV in percentages (lower is better), the following observations are possible:

- With default settings and image exclusion, the impact on response time is between 53 and 60%
- When fully optimized, the impact on response time is around 25% for both the stateful and stateless configurations.

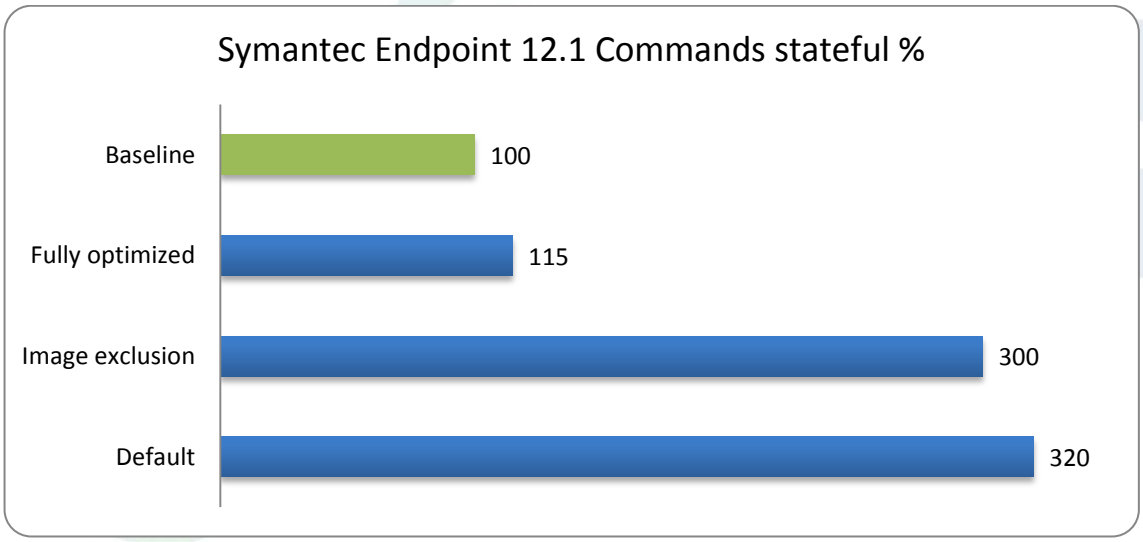


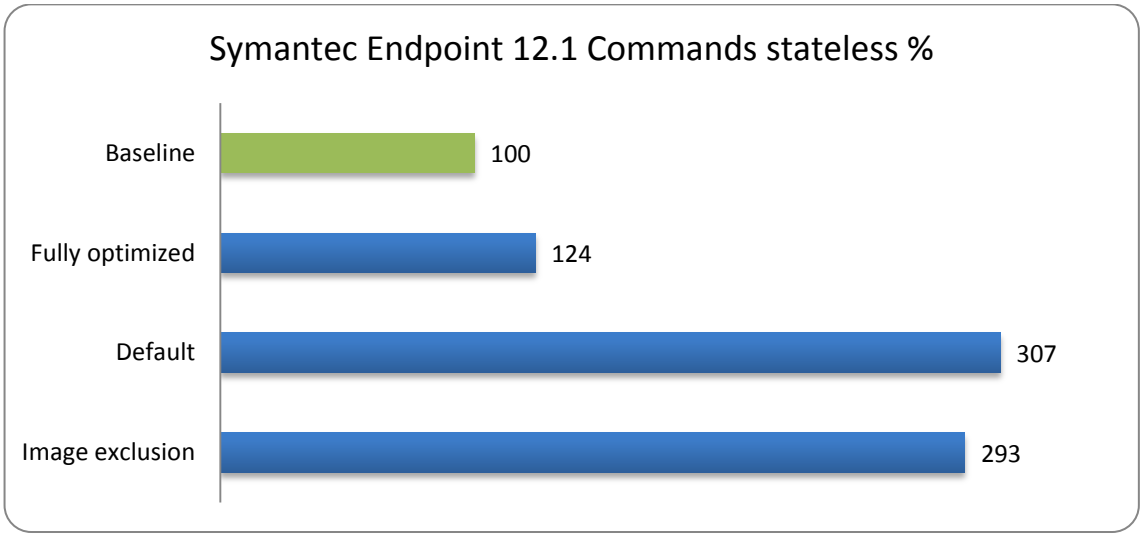


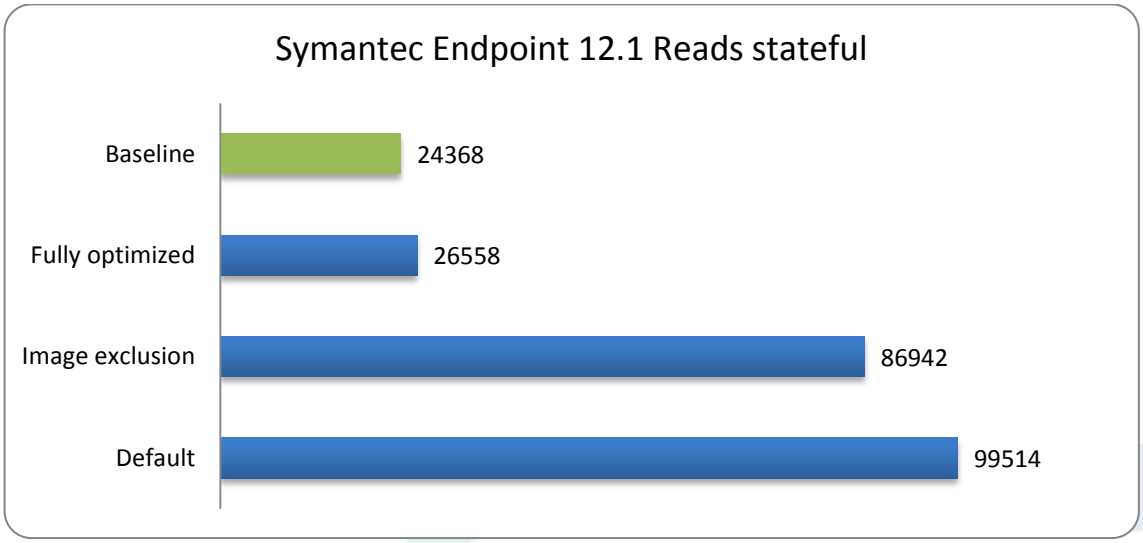
12.3 DISK IO RESULTS

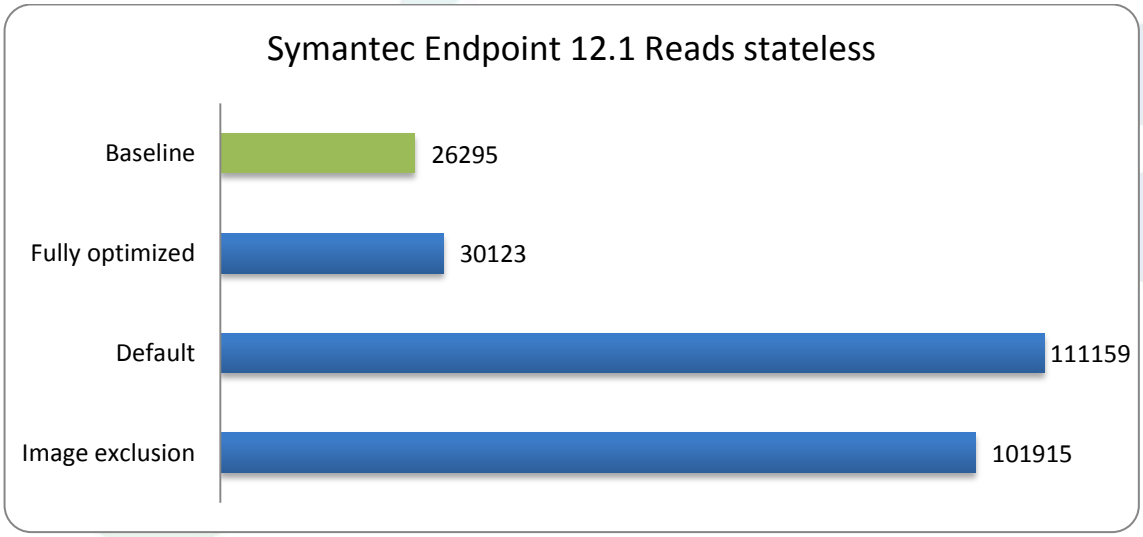
Reviewing disk IO total command (including total reads and writes) results, when 50 Login VSI sessions are logged on (lower is better), the following observations are possible:

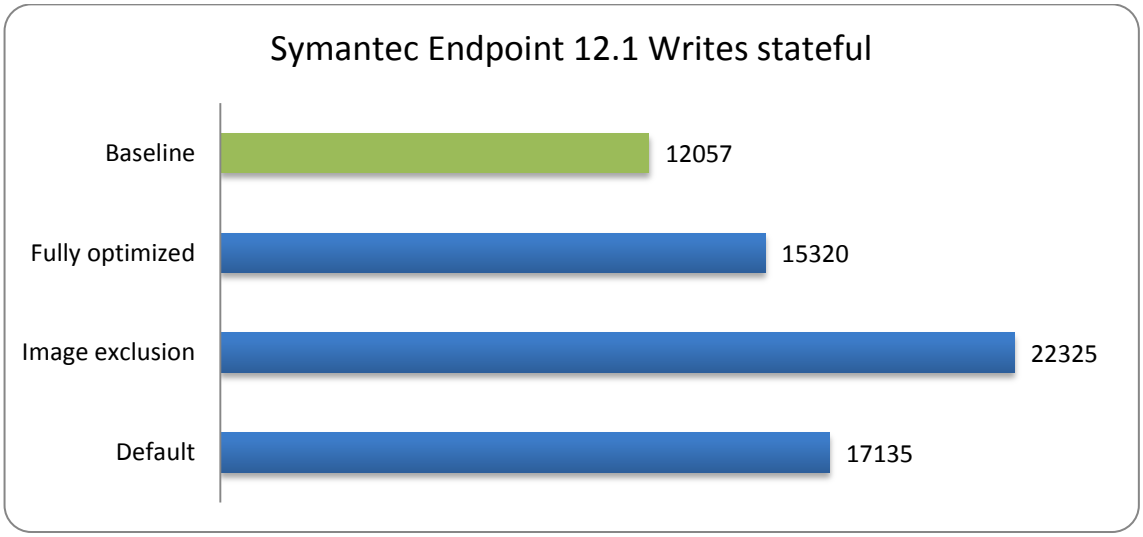
- With default settings and image exclusion, the impact on disk IO is high: around 200% higher than baseline.
- However, when Symantec is fully optimized for performance, the impact is 15% for stateful and 24% for stateless.
- When the read and the write IO's are compared, it is clear that most overhead comes from the read IO's.

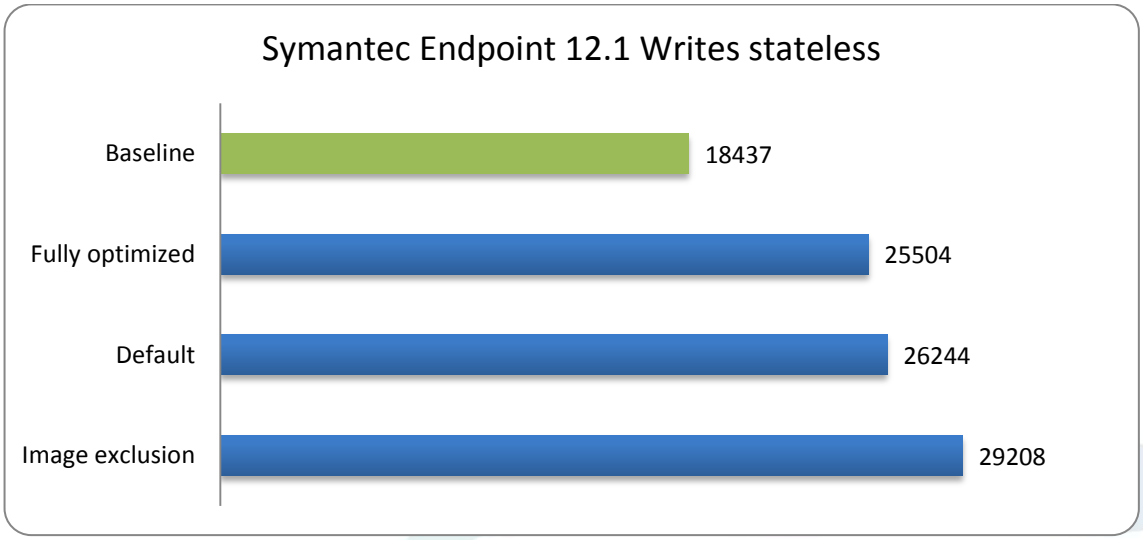



Symantec Endpoint 12.1 Commands stateless %
Baseline
100
Fully optimized
124
Default
307
Image exclusion
293


Symantec Endpoint 12.1 Reads stateful
Baseline
24368
Fully optimized
26558
Image exclusion
86942
Default
99514


Symantec Endpoint 12.1 Reads stateless
Baseline
26295
Fully optimized
30123
Default
111159
Image exclusion
101915

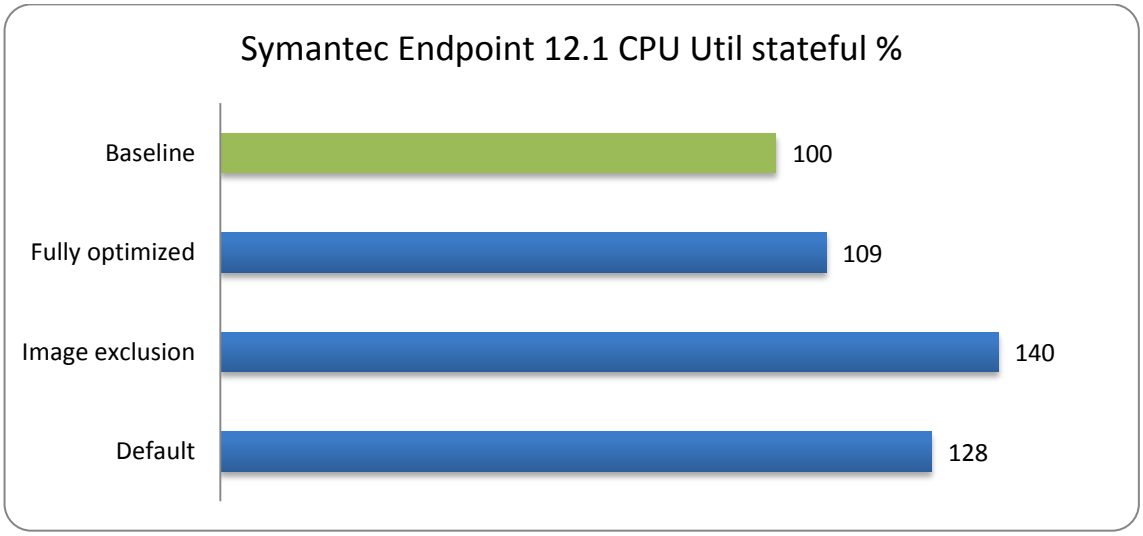


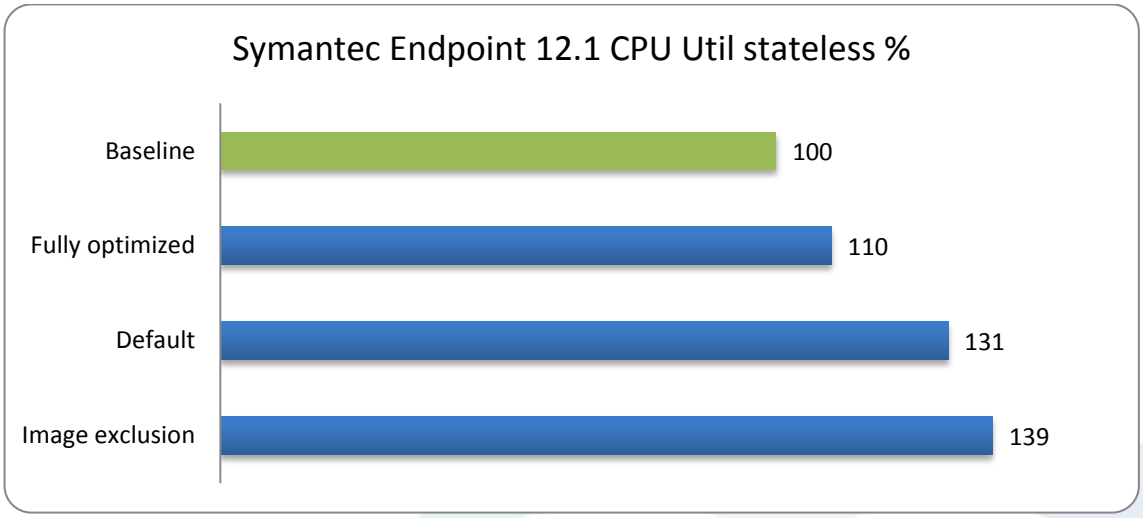


12.4 CPU UTILIZATION WITH 50 SESSIONS

Reviewing the average total Processor Utilization, when 50 Login VSI sessions are logged on (lower is better), the following observations are possible:

- With default settings and image exclusion, the average CPU utilization ranges from 28% to 40% impact in comparison to the baseline without AV.
- Fully optimized the impact of Symantec is reduced around 10% for both stateful and stateless configurations.


Symantec Endpoint 12.1 CPU Util stateful %
Baseline
100
Fully optimized
109
Image exclusion
140
Default
128


Symantec Endpoint 12.1 CPU Util stateless %
Baseline
100
Fully optimized
110
Default
131
Image exclusion
139

12.5 OVERVIEW OF SETTINGS

Fully Optimized		
Configuration	***Setting***	***Description***
Virus and Spyware protection policy/scheduled scan through policy	Disabled	Disable scheduled scans.
Virus and Spyware protection policy/Run an Active Scan when new definitions arrive	Disabled	Disable running an active scan when new definitions arrive.
Virus and Spyware protection policy/Specify actions that trigger automatic scans	Scan when a file is modified	Only scan files when written to.
Virus and Spyware protection policy/Scan files on remote computers	Disabled	Do not scan files on remote computers.
Virus and Spyware protection policy/SONAR/TruScan	Disabled	Disable SONAR and TruScan behavioral monitoring.
Virus and Spyware protection policy/Bloodhound	Disabled	Disable Bloodhound behavioral monitoring.
Virus and Spyware protection policy/Download insight	Disabled	Do not scan downloaded files.
Virus and Spyware protection policy/Email plugins (Internet Email, Outlook, Lotus Notes)	Disabled	Disable email plugins
Virus and Spyware protection policy/Virtual Image Exception	Enabled	Use the Virtual Image Exception technology. This tool allows to exclude all the files on a baseline image from scanning.
LiveUpdate settings policy/Use a LiveUpdate server	Disabled	Do not use the LiveUpdate server to get definition updates.
LiveUpdate content policy/Use specific revision	Enabled	Use the revision that was current when the software was installed.
Exceptions policy	"C:\Program Files\Login Consultants\VSI"	Disable scanning for files under the paths specified.
Exceptions policy	B:\	Disable scanning for files under the paths specified.
Exceptions policy	G:\	Disable scanning for files under the paths specified.
Exceptions policy	H:\	Disable scanning for files under the paths specified.
Intrusion Prevention policy/Enable Intrusion Prevention	Disabled	Disables the intrusion prevention system engine that checks IPS signatures, exceptions to IPS signatures, and custom signatures.
ClientSideClonePreperationTool	http://www.symantec.com/business/support/index?page=content&id=HOWTO54706	This tool will remove all Symantec Endpoint Protection client identifiers and leave the Endpoint Protection services stopped. It should be done as the last step in the image preparation process, before running sysprep and/or shutting down the system
Following features are disabled since they aren't installed on the client		
Download protection		
Microsoft Outlook scanner		
Lotus Notes scanner		
POP3/SMTP scanner		
Proactive Threat protection		
SONAR protection		
Application and device control		
Network threat protection		

Intrusion protection		
Firewall		
Shared Insight Cache is only available for the clients that perform scheduled scans and manual scans.		
Default		
Configuration	***Setting***	***Description***
Virus and Spyware protection policy/scheduled scan through policy	Disabled	Disable scheduled scans.
Virus and Spyware protection policy/Run an Active Scan when new definitions arrive	Disabled	Disable running an active scan when new definitions arrive.
LiveUpdate settings policy/Use a LiveUpdate server	Disabled	Do not use the LiveUpdate server to get definition updates.
LiveUpdate content policy/Use specific revision	Enabled	Use the revision that was current when the software was installed.
Exceptions policy	"C:\Program Files\Login Consultants\VSI"	Disable scanning for files under the paths specified.
Exceptions policy	B:\	Disable scanning for files under the paths specified.
Exceptions policy	G:\	Disable scanning for files under the paths specified.
Exceptions policy	H:\	Disable scanning for files under the paths specified.
ClientSideClonePreperationTool	http://www.symantec.com/business/support/index?page=content&id=HOWTO54706	This tool will remove all Symantec Endpoint Protection client identifiers and leave the Endpoint Protection services stopped. It should be done as the last step in the image preparation process, before running sysprep and/or shutting down the system

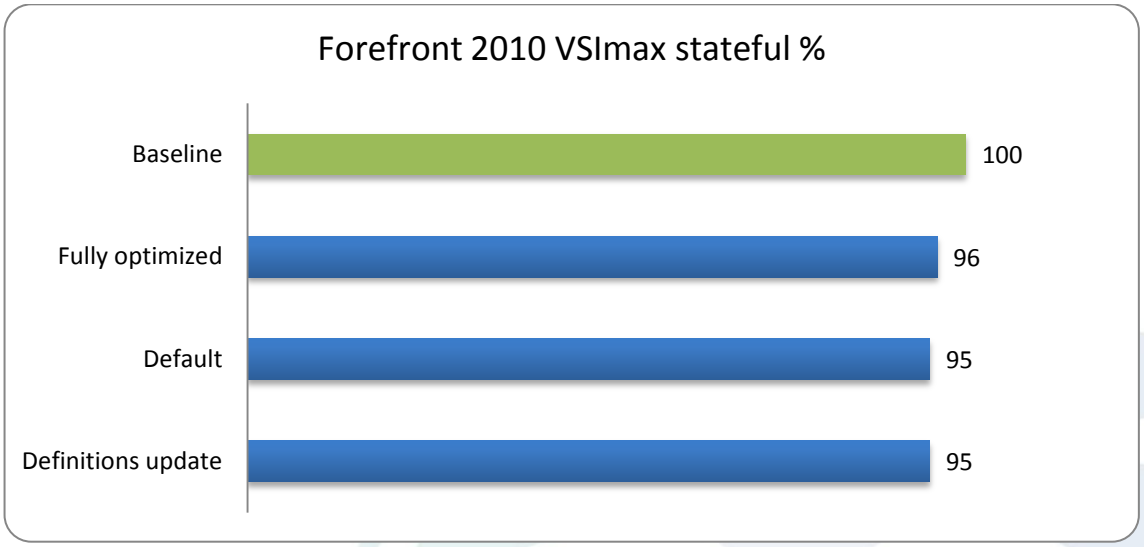
13. MICROSOFT FOREFRONT ENDPOINT PROTECTION 2010

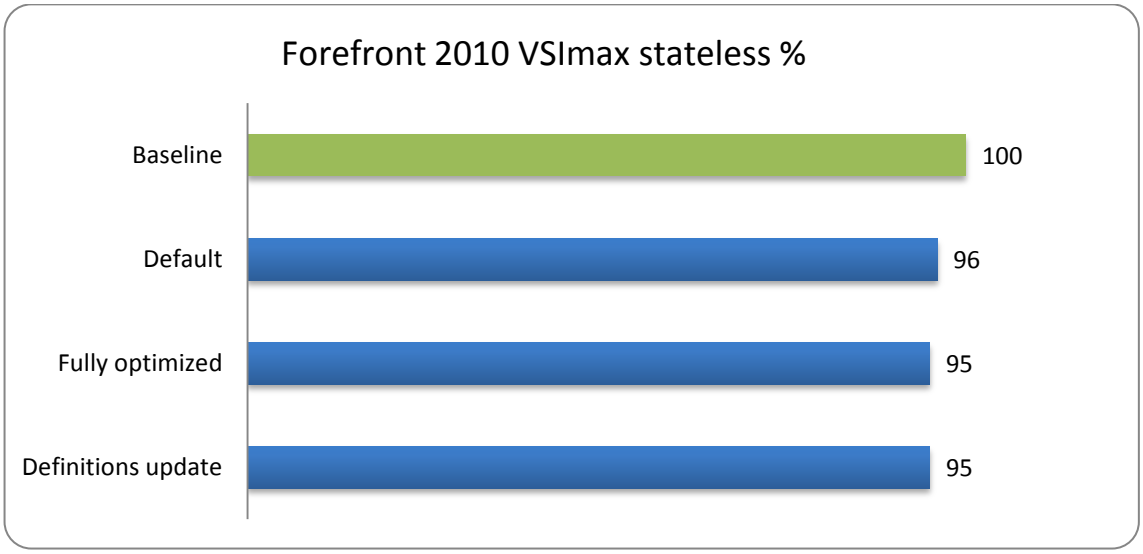
Microsoft Forefront Endpoint Protection is a conventional AV solution. After McAfee, Symantec and Trend Micro, Microsoft Forefront is used by 14% of the Project VRC survey participants.

13.1 VSIMAX RESULTS

Reviewing the VSImax results in comparison to the baseline results without AV in percentages (higher is better), the following observations are possible:

- Optimization do not affect VSImax. All results, including default show a 5% capacity impact.
- There is no difference in impact with stateful and stateless desktop VM's.
- A definition update did not change the impact it has on VSImax.

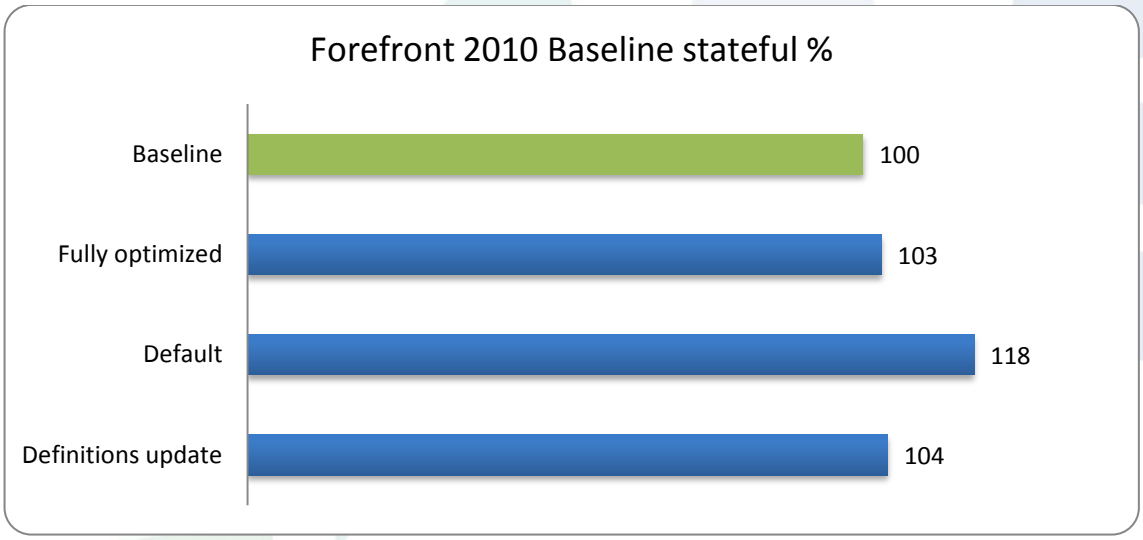


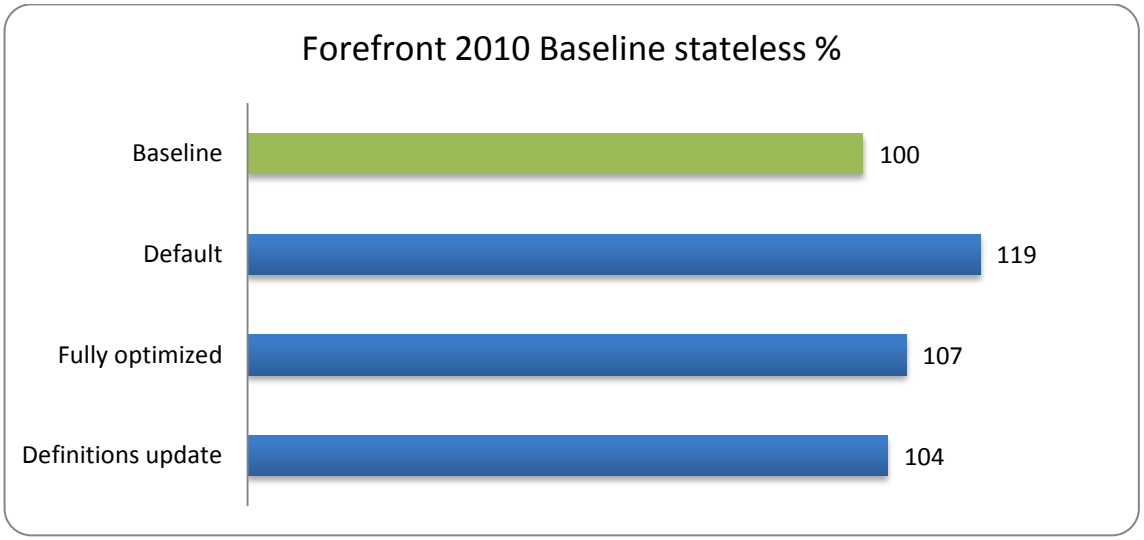


13.2 BASELINE LOGIN VSI RESPONSE TIME RESULTS

Reviewing baseline response time for the VSImax results in comparison to the baseline results without AV in percentages (lower is better), the following observations are possible:

- The response time with default setting is increased by around 18% for both the stateful and stateless tests.
- Fully optimized and after a definition update, the overhead on the Login VSI response time is between 3% and 7%.

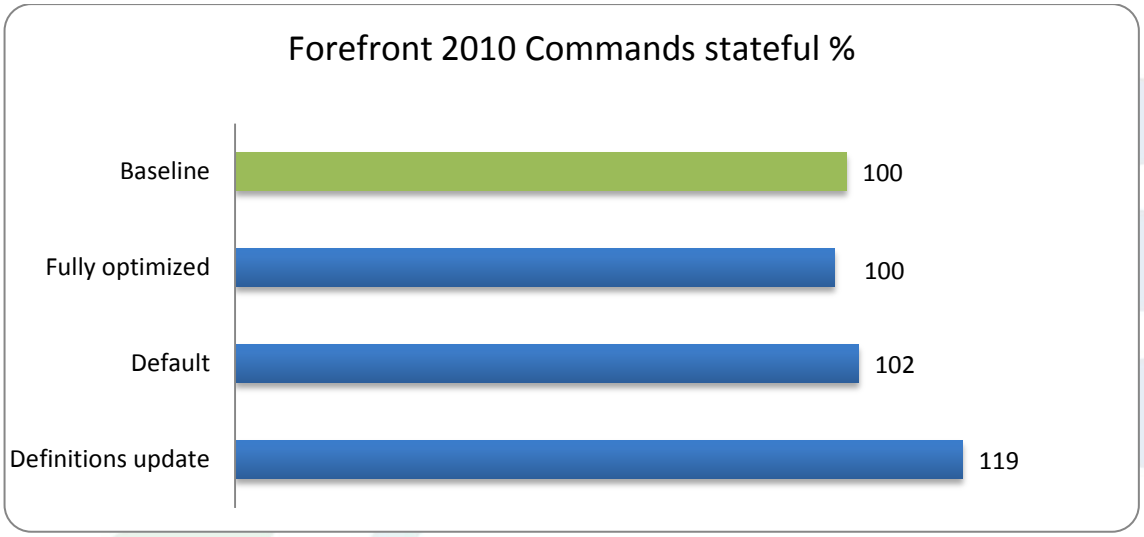


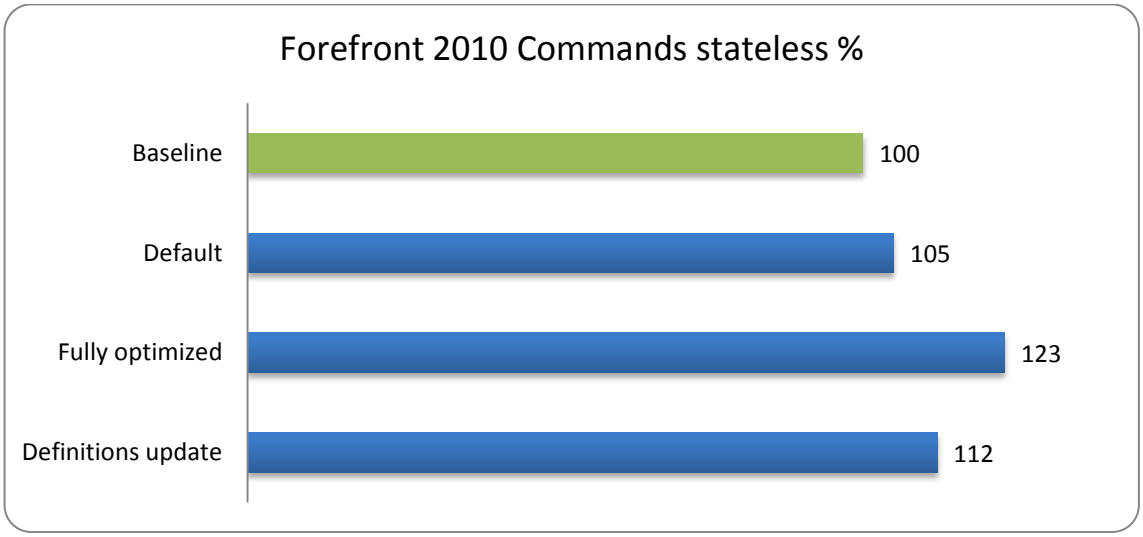


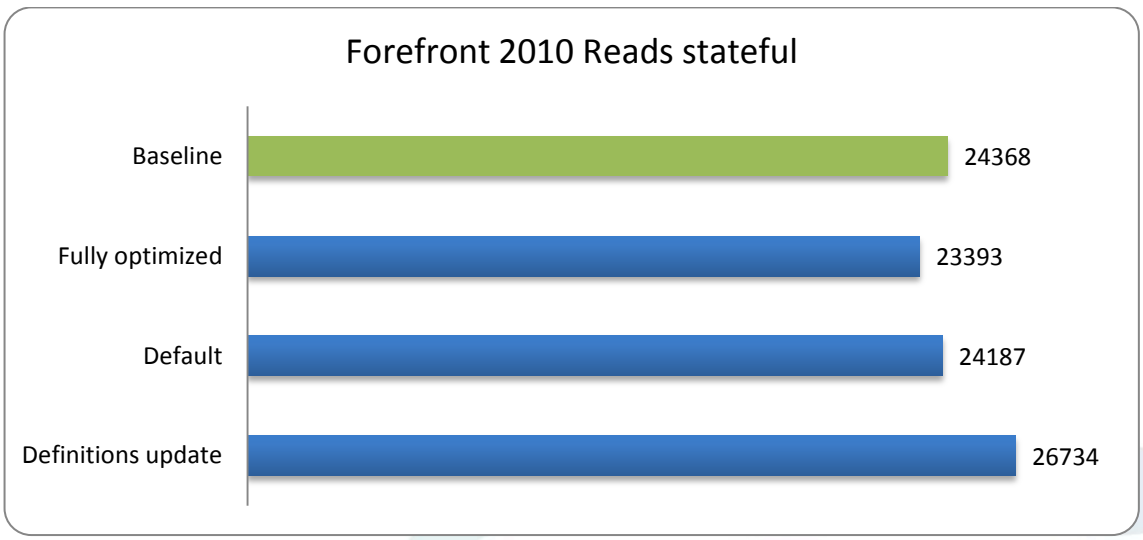
13.3 DISK IO RESULTS

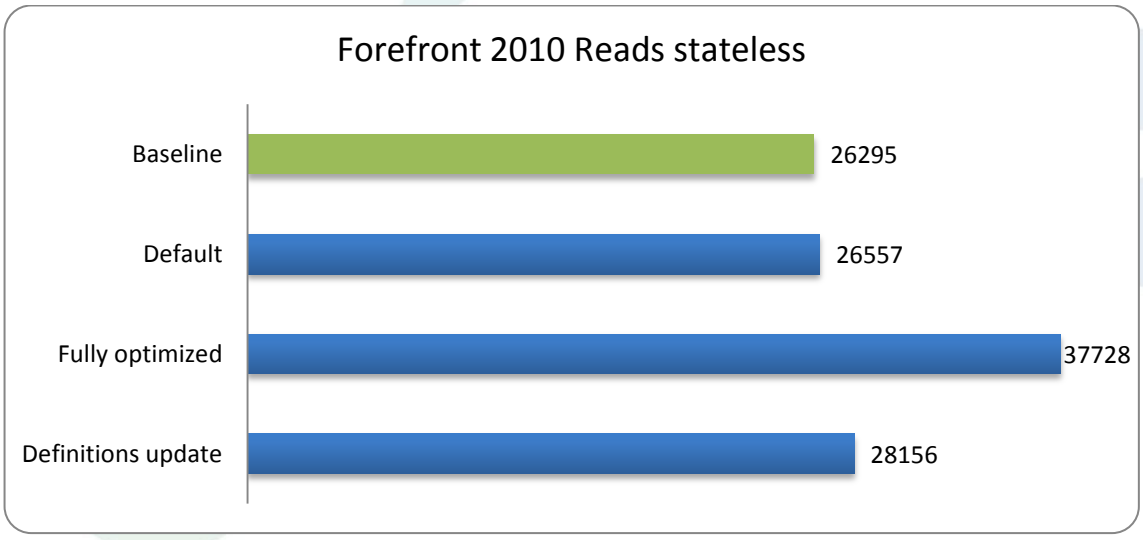
Reviewing disk IO total command (including total reads and writes) results, when 50 Login VSI sessions are logged on (lower is better), the following observations are possible:

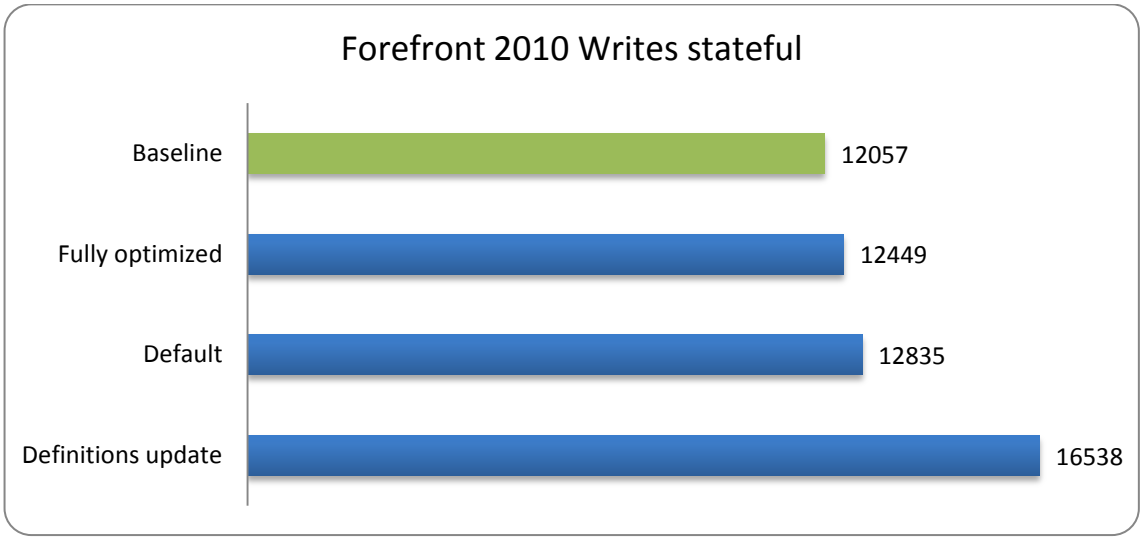
- For all tests the total IO overhead is minimal, ranging from no to about 23% overhead.

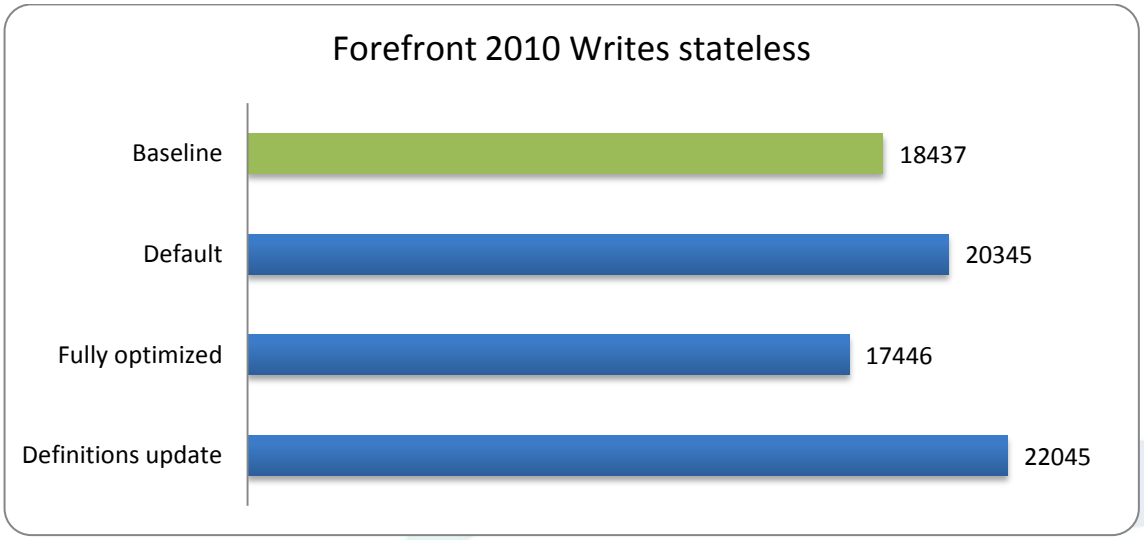



Forefront 2010 Commands stateless %
Baseline
100
Default
105
Fully optimized
123
Definitions update
112


Forefront 2010 Reads stateful
Baseline
24368
Fully optimized
23393
Default
24187
Definitions update
26734


Forefront 2010 Reads stateless
Baseline
26295
Default
26557
Fully optimized
37728
Definitions update
28156

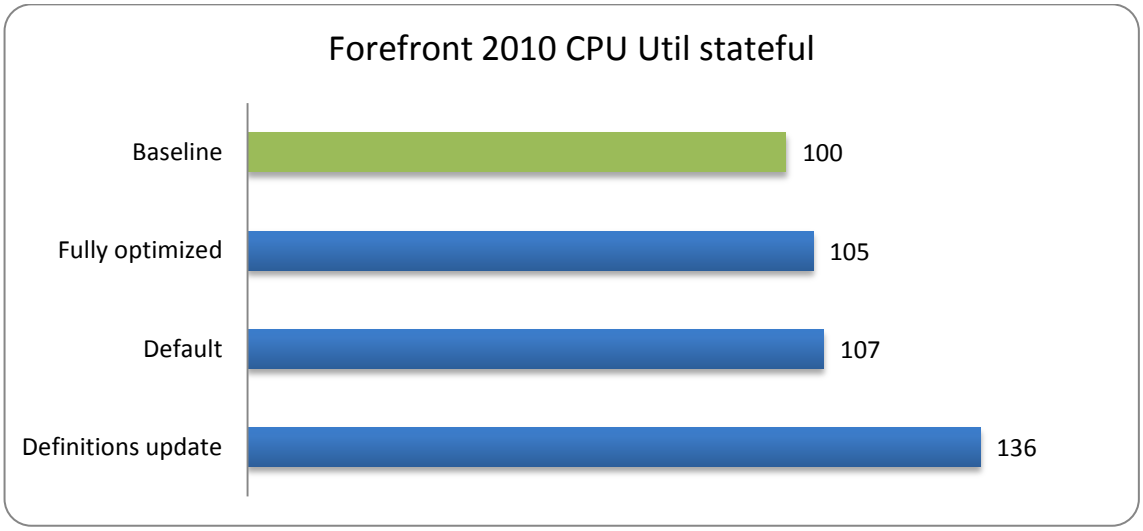


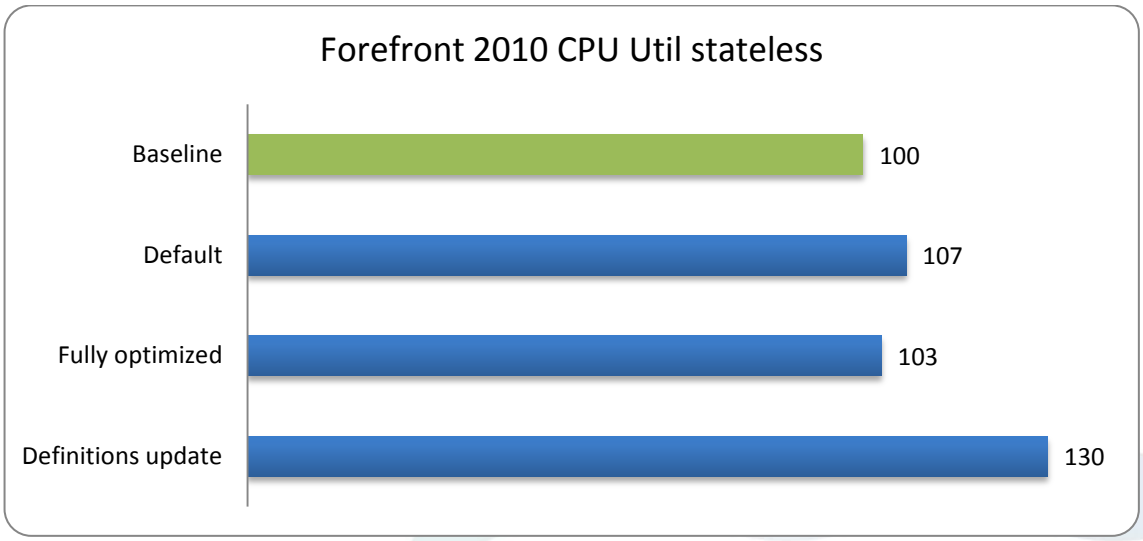


13.4 CPU UTILIZATION WITH 50 SESSIONS

Reviewing the average total Processor Utilization, when 50 Login VSI sessions are logged on (lower is better), the following observations are possible:

- For both the default and fully optimized configurations, the CPU overhead at 50 sessions is minimal, ranging from 3% to 7%.
- Interestingly, the CPU overhead is considerably higher with a definition update, ranging from 30% (stateless) to 36% with stateful configurations.


Forefront 2010 CPU Util stateful
Baseline
100
Fully optimized
105
Default
107
Definitions update
136


Forefront 2010 CPU Util stateless
Baseline
100
Default
107
Fully optimized
103
Definitions update
130

13.5 OVERVIEW OF SETTINGS

Fully Optimized		
Configuration	***Setting***	***Description***
System/Forefront Endpoint Protection 2010/Exclusions/Path Exclusions	"C:\Program Files\Login Consultants\VSI"	Disable scheduled and real-time scanning for files under the paths specified.
System/Forefront Endpoint Protection 2010/Exclusions/Path Exclusions	B:\	Disable scheduled and real-time scanning for files under the paths specified.
System/Forefront Endpoint Protection 2010/Exclusions/Path Exclusions	G:\	Disable scheduled and real-time scanning for files under the paths specified.
System/Forefront Endpoint Protection 2010/Exclusions/Path Exclusions	H:\	Disable scheduled and real-time scanning for files under the paths specified.
System/Forefront Endpoint Protection 2010/Real-time Protection/Configure monitoring for incoming and outgoing file and program activity	scan only incoming (disable on-open)	This policy setting allows you to configure monitoring for incoming and outgoing files, without having to turn off monitoring entirely.
System/Forefront Endpoint Protection 2010/Real-time Protection/Turn on behavior monitoring	Disabled	If you disable this setting, behavior monitoring will be disabled.
System/Forefront Endpoint Protection 2010/Remediation/Specify the time of day to run a scheduled full scan to complete remediation	Disabled	This policy setting allows you to specify the time of day at which to perform a scheduled full scan in order to complete remediation.
System/Forefront Endpoint Protection 2010/Scan/Check for the latest virus and spyware definitions before running a scheduled scan	Disabled	If you disable this setting or do not configure this setting, the scan will start using the existing definitions.
System/Forefront Endpoint Protection 2010/Scan/Configure local setting override for schedule scan day	Disabled	If you disable or do not configure this setting, Group Policy will take priority over the local preference setting.
System/Forefront Endpoint Protection 2010/Scan/Configure local setting override for scheduled quick scan time	Disabled	If you disable or do not configure this setting, Group Policy will take priority over the local preference setting.
System/Forefront Endpoint Protection 2010/Scan/Specify the time for a daily quick scan	Disabled	This policy setting allows you to specify the time of day at which to perform a daily quick scan.
System/Forefront Endpoint Protection 2010/Scan/Specify the time of day to run a scheduled scan	Disabled	This policy setting allows you to specify the time of day at which to perform a scheduled scan
System/Forefront Endpoint Protection 2010/Scan/Start the scheduled scan only when computer is on but not in use	Disabled	If you disable this setting, scheduled scans will run at the scheduled time.
System/Forefront Endpoint Protection 2010/Scan/Turn on heuristics	Disabled	If you disable this setting, heuristics will be disabled.
System/Forefront Endpoint Protection 2010/Signature Updates/Specify the day of the week to check for definition updates	Enabled: Never	This policy setting allows you to specify the day of the week on which to check for definition updates.
System/Forefront Endpoint Protection 2010/Signature Updates/Specify the time to check for definition updates	Disabled	This policy setting allows you to specify the time of day at which to check for definition updates
Default		
Configuration	***Setting***	***Description***
System/Forefront Endpoint Protection 2010/Exclusions/Path Exclusions	"C:\Program Files\Login Consultants\VSI"	Disable scheduled and real-time scanning for files under the paths specified.
System/Forefront Endpoint Protection 2010/Exclusions/Path Exclusions	B:\	Disable scheduled and real-time scanning for files under the paths specified.
System/Forefront Endpoint Protection 2010/Exclusions/Path Exclusions	G:\	Disable scheduled and real-time scanning for files under the paths specified.
System/Forefront Endpoint Protection 2010/Exclusions/Path Exclusions	H:\	Disable scheduled and real-time scanning for files under the paths specified.
System/Forefront Endpoint Protection 2010/Remediation/Specify the time of day to run a scheduled full scan to complete remediation	Disabled	This policy setting allows you to specify the time of day at which to perform a scheduled full scan in order to complete remediation.
System/Forefront Endpoint Protection 2010/Scan/Check for the latest virus and spyware definitions before running a scheduled scan	Disabled	If you disable this setting or do not configure this setting, the scan will start using the existing definitions.
System/Forefront Endpoint Protection 2010/Scan/Configure local setting override for schedule scan day	Disabled	If you disable or do not configure this setting, Group Policy will take priority over the local preference setting.
System/Forefront Endpoint Protection 2010/Scan/Configure local setting override for scheduled quick scan time	Disabled	If you disable or do not configure this setting, Group Policy will take priority over the local preference setting.

System/Forefront Endpoint Protection 2010/Scan/Specify the time for a daily quick scan	Disabled	This policy setting allows you to specify the time of day at which to perform a daily quick scan.
System/Forefront Endpoint Protection 2010/Scan/Specify the time of day to run a scheduled scan	Disabled	This policy setting allows you to specify the time of day at which to perform a scheduled scan
System/Forefront Endpoint Protection 2010/Scan/Start the scheduled scan only when computer is on but not in use	Disabled	If you disable this setting, scheduled scans will run at the scheduled time.
System/Forefront Endpoint Protection 2010/Signature Updates/Specify the day of the week to check for definition updates	Enabled: Never	This policy setting allows you to specify the day of the week on which to check for definition updates.
System/Forefront Endpoint Protection 2010/Signature Updates/Specify the time to check for definition updates	Disabled	This policy setting allows you to specify the time of day at which to check for definition updates

14. COMPARING DEFAULT ON VMWARE VSPHERE

The comparisons in the following charts should not come as a surprise: the results have already been described and reviewed in the previous chapters. It's difficult to compare AV solutions from a performance impact perspective because they are functionally and technically so different. Therefore we have chosen to only compare the results using a default configuration and the tests where image exclusion is set. Both configurations should not be controversial with most security officers.

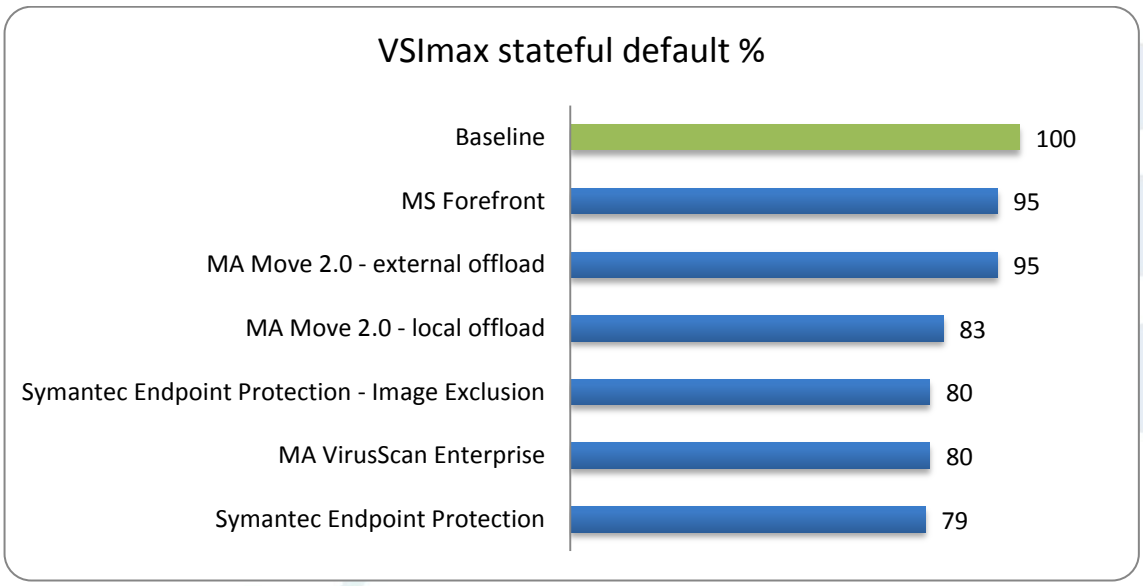
McAfee MOVE 2.5 agentless is not compared to other solutions because it was tested on vSphere 5.0 instead of vSphere 4.1.

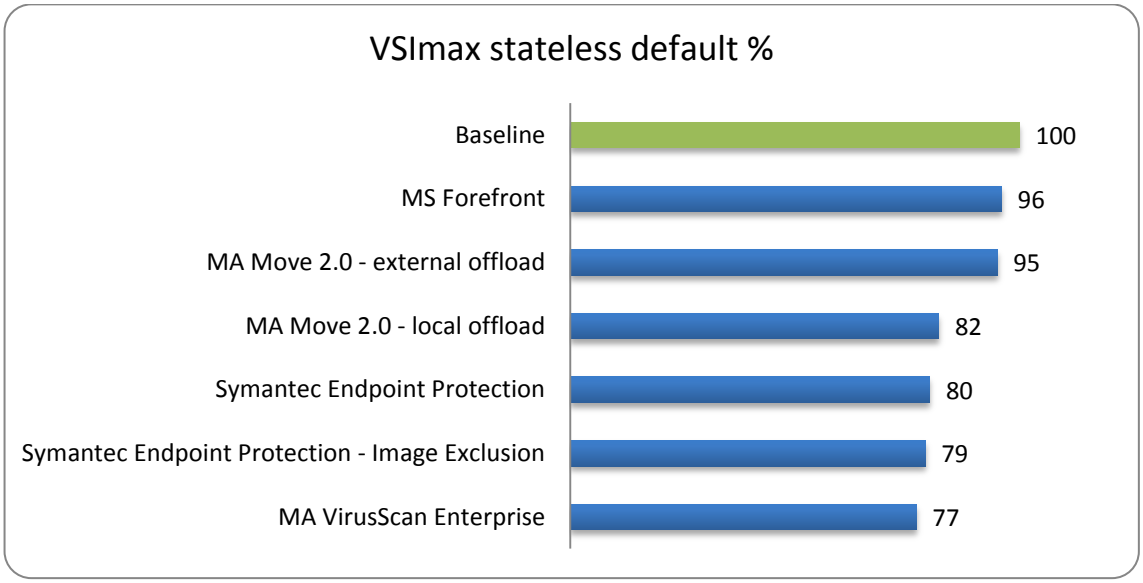
It's clear that Microsoft Forefront has the least overhead in our test. This is only the case were the pre-scan was performed of the master image before deployment in the pool. Without such a pre-scan Forefront performance impact would be enormous in comparison.

McAfee MOVE 2.0 – external offload is second in the chart, but this comparison is not fair to the other solutions, as the offloading VM is running on a physically different host.

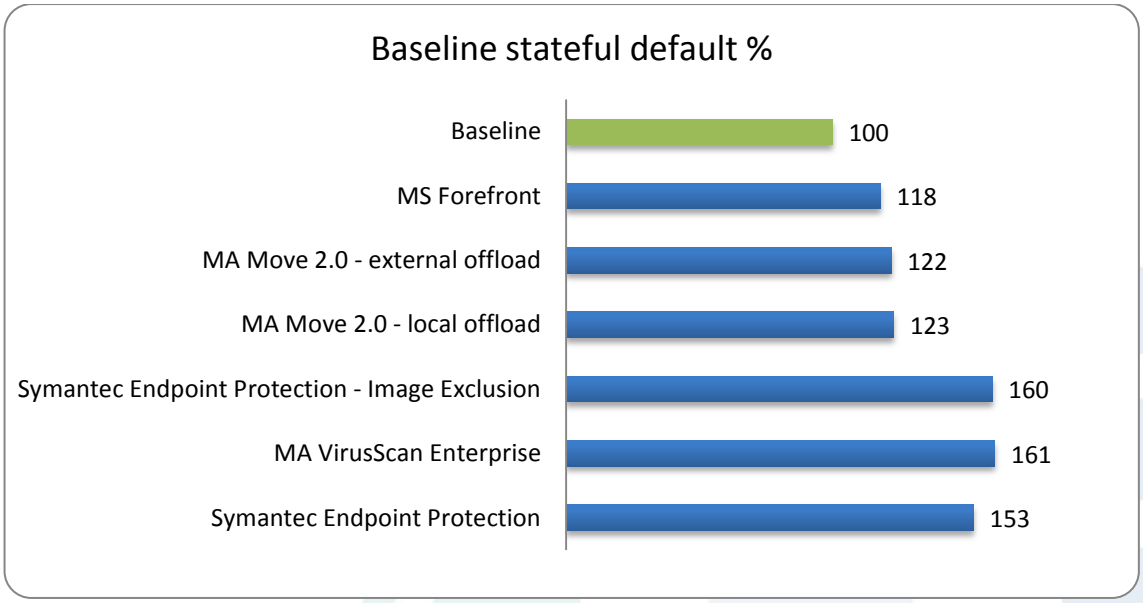
It is already mentioned a couple times in this document, but Project VRC cannot comment on the quality of the AV solution, this has never been the objective of the research.

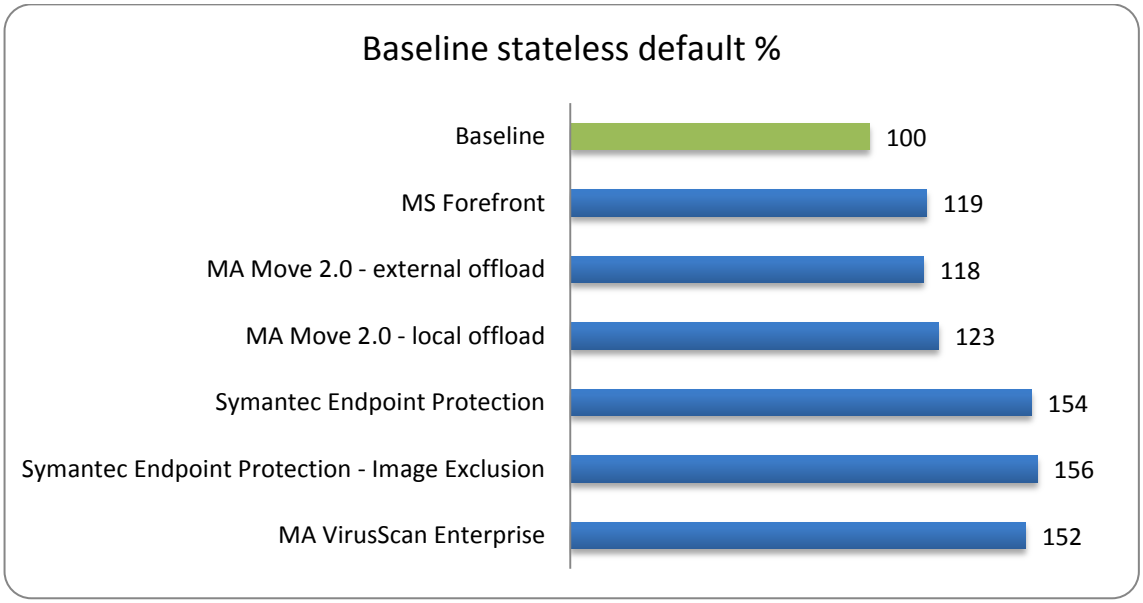
14.1 VSIMAX COMPARISONS VSPHERE 4.1



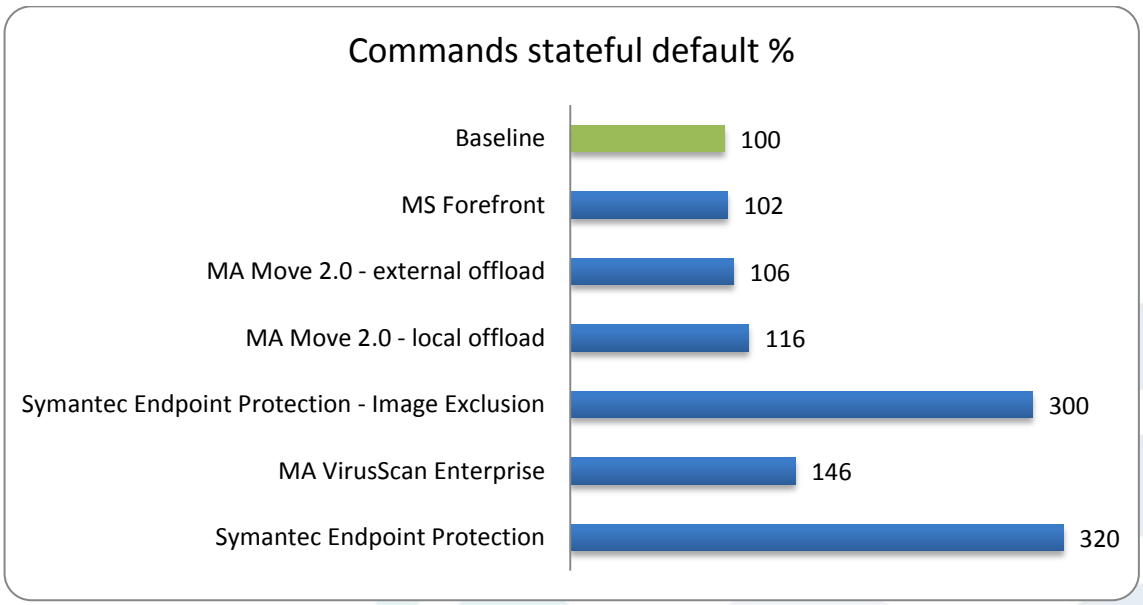


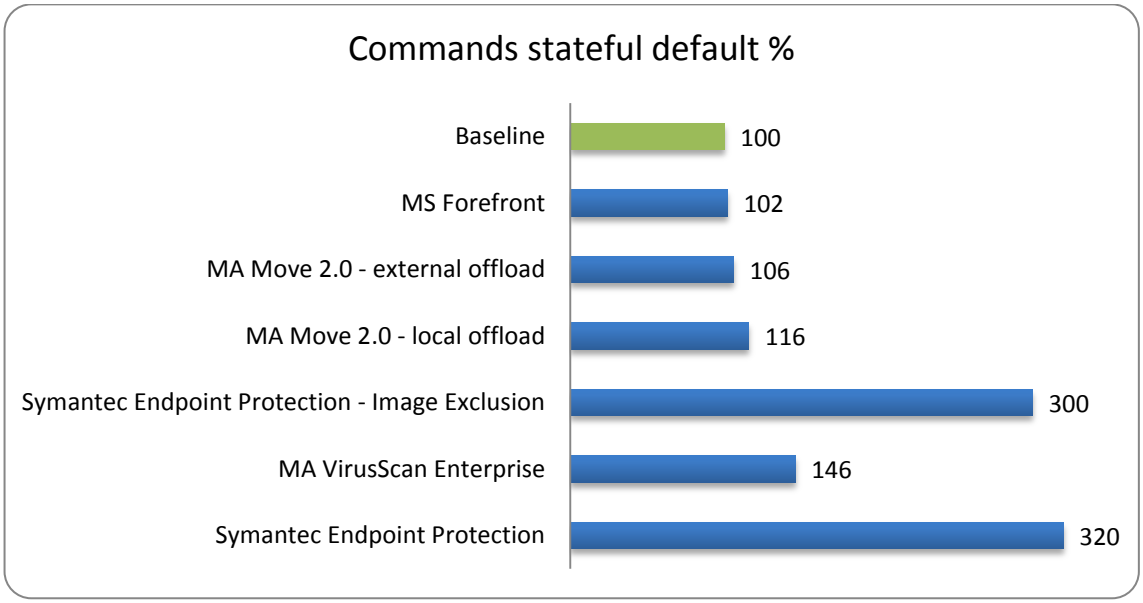
14.2 BASELINE LOGIN VSI RESPONSE TIME COMPARISONS VSPHERE 4.1



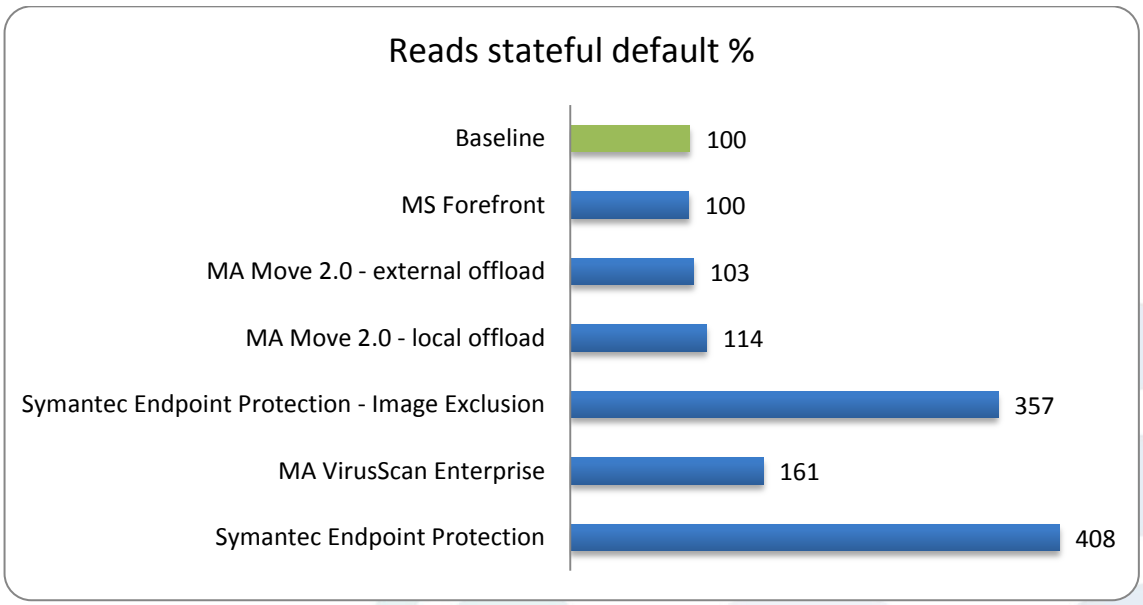


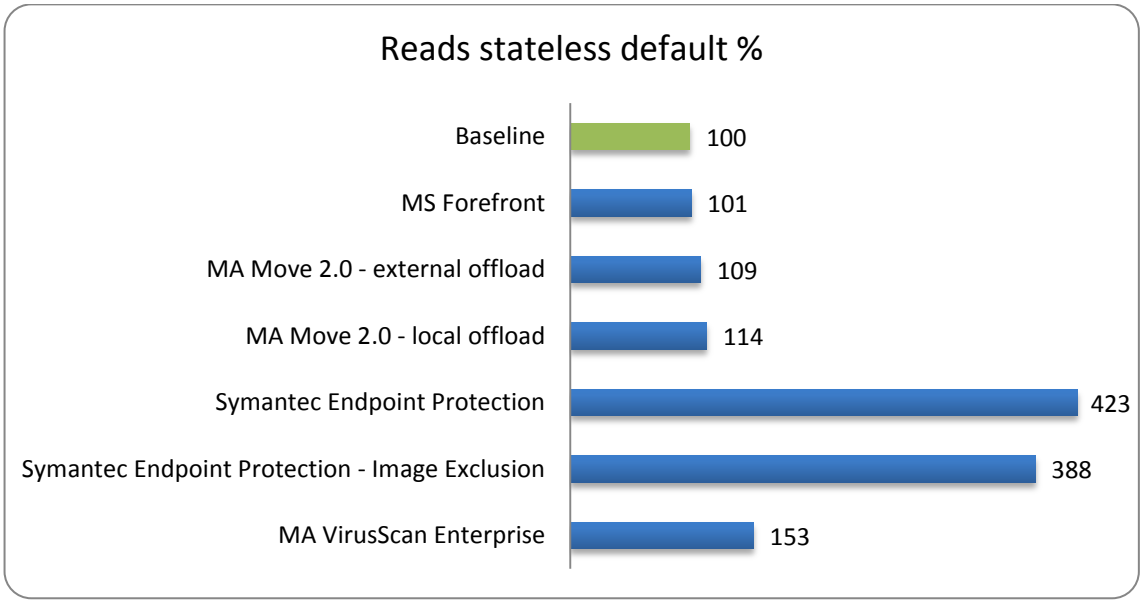
14.3 DISK IO TOTAL COMMANDS @ 50 SESSIONS COMPARISONS VSPHERE 4.1

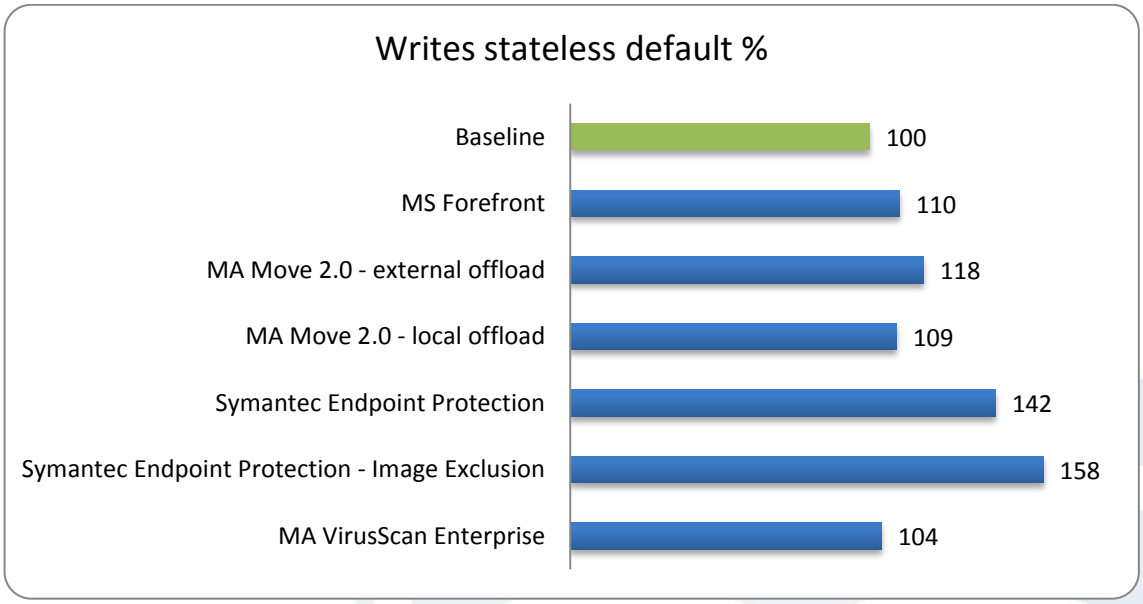




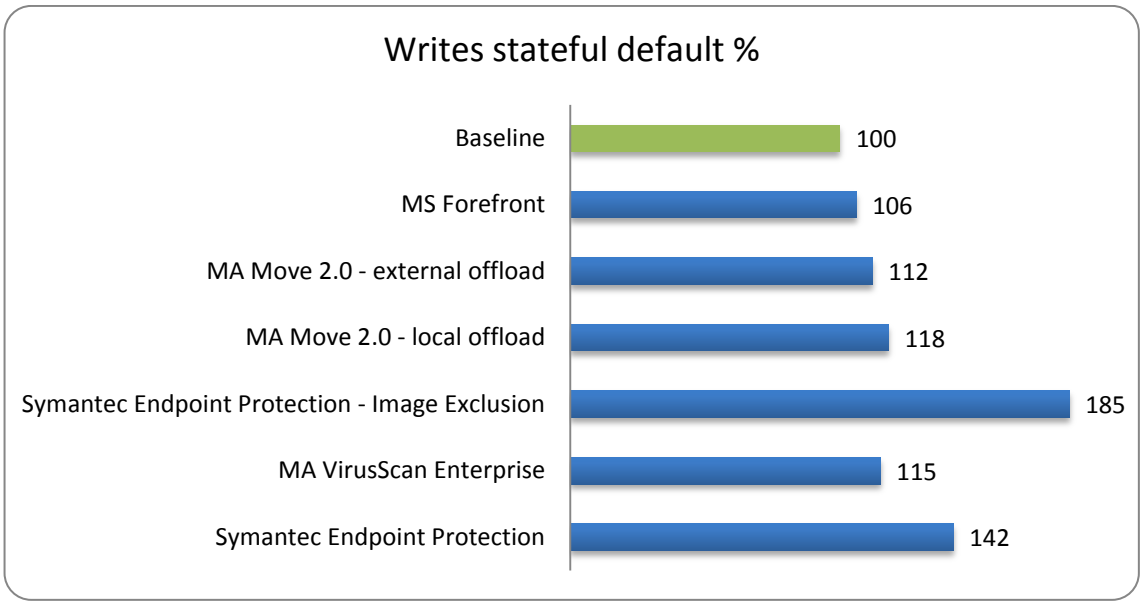
14.4 DISK IO READ COMMANDS @ 50 SESSIONS COMPARISONS VSPHERE 4.1



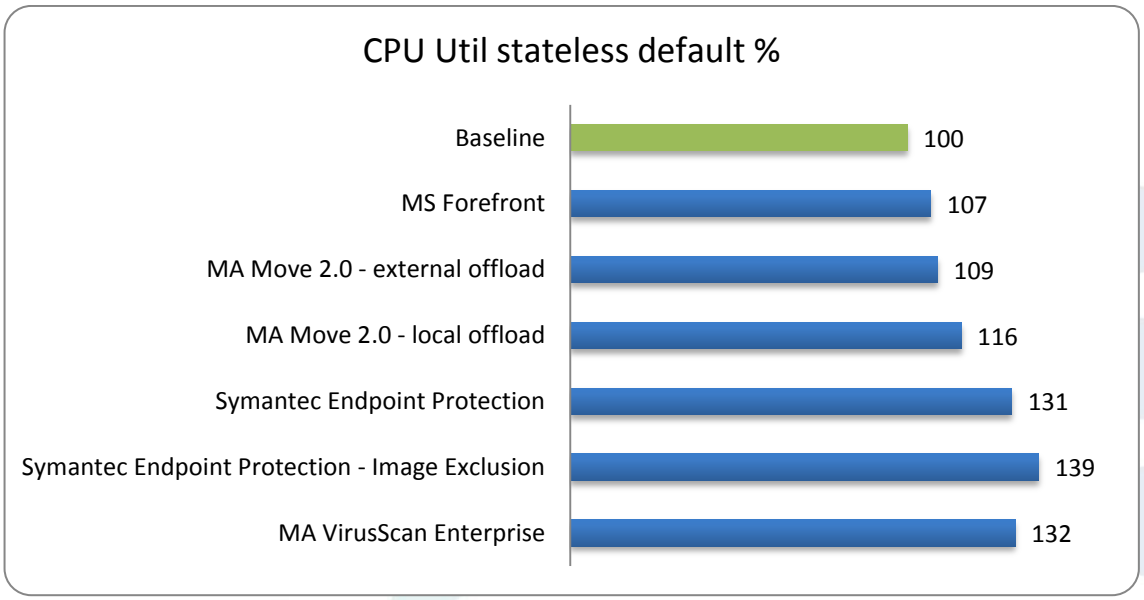

Reads stateless default %
Baseline
100
MS Forefront
101
MA Move 2.0 - external offload
109
MA Move 2.0 - local offload
114
Symantec Endpoint Protection
423
Symantec Endpoint Protection - Image Exclusion
388
MA VirusScan Enterprise
153

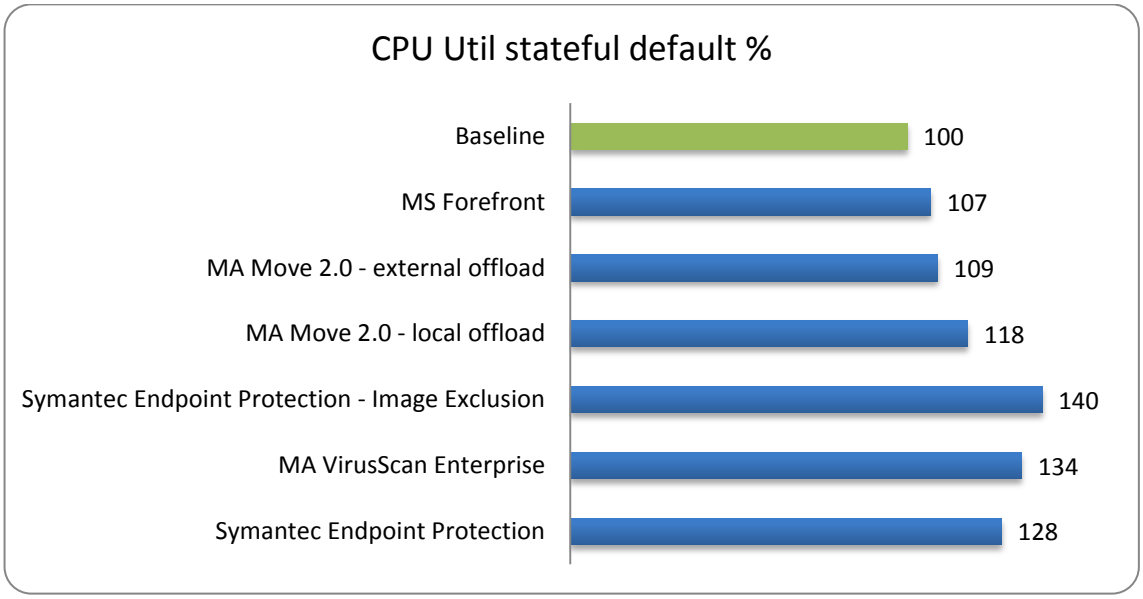

Writes stateless default %
Baseline
100
MS Forefront
110
MA Move 2.0 - external offload
118
MA Move 2.0 - local offload
109
Symantec Endpoint Protection
142
Symantec Endpoint Protection - Image Exclusion
158
MA VirusScan Enterprise
104

14.5 DISK IO WRITE COMMANDS @ 50 SESSIONS COMPARISONS VSPHERE 4.1



14.6 CPU AVERAGE UTILIZATION @ 50 SESSIONS COMPARISONS VSPHERE 4.1




CPU Util stateful default %
Baseline
100
MS Forefront
107
MA Move 2.0 - external offload
109
MA Move 2.0 - local offload
118
Symantec Endpoint Protection - Image Exclusion
140
MA VirusScan Enterprise
134
Symantec Endpoint Protection
128

Login Consultant B.V.
De Entree 11-13
1101 BH Amsterdam
The Netherlands

Tel: +31 (0)20 3420280
Fax: +31 (0)20 6975721
E-mail: info@loginconsultants.nl
www.loginconsultants.com

Eenvoud in ICT

PQR B.V.
Rijnzathe 7
3454 PV De Meern
The Netherlands

Tel: +31 (0)30 6629729
Fax: +31 (0)30 6665905
E-mail: info@pqr.nl
www.pqr.com