TEST REPORT

Tolly.

#214110

April 2014

Commissioned by Sophos Ltd.

Sophos Antivirus for vShield v1.0

VMware Server and VDI Client Application Performance versus Trend Micro Deep Security and McAfee MOVE Agentless

EXECUTIVE SUMMARY

A key element in the explosive growth of virtualization is the ability to drive the physical server hardware to higher, and more cost-efficient, utilization levels. With that in mind, it is important that server resources are not wasted by overly demanding antivirus (AV) solutions. VMware's vShield Endpoint™ provides access to VM resources via a virtual appliance rather than by requiring agents on each VM.

Sophos commissioned Tolly to evaluate its Antivirus for vShield v1.0 solution and compare its performance to two other vShield-based offerings: McAfee MOVE Agentless 3.0 and Trend Micro Deep Security 9. Tests encompassed a range of VMware ESXi 5.5 Microsoft Server 2008 virtual server applications including a web, database and file services. A virtual desktop infrastructure (VDI) environment with 120 Windows 7 Enterprise virtual machines on a host was also evaluated using a VMware View Planner 2.1 standard workload.

The Sophos solution demonstrated consistently better performance and, by inference, lower system resource demands than the McAfee and Trend Micro solutions. See Figures 1 and 2. < Continued on next page >

THE BOTTOM LINE

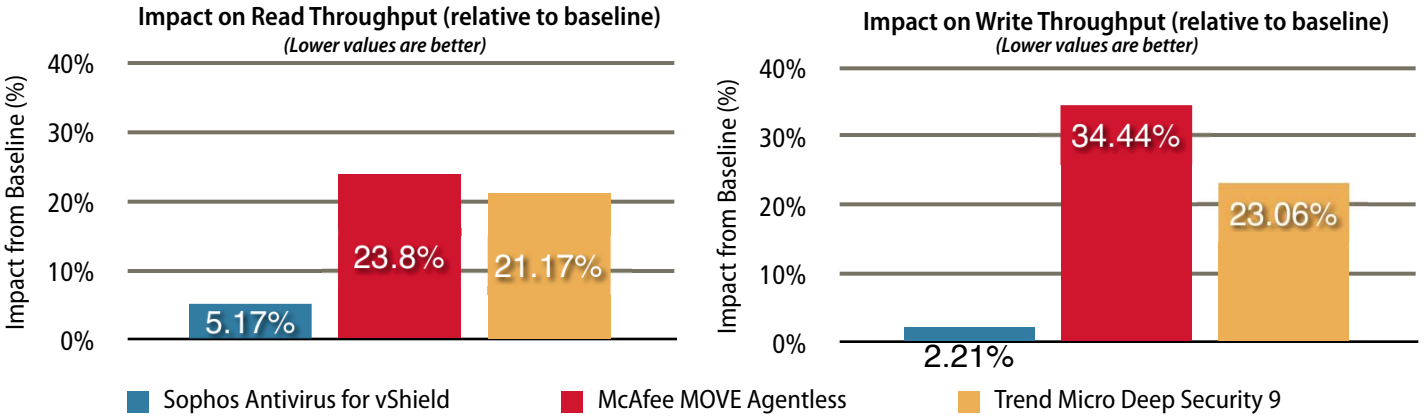
Sophos Antivirus for vShield 1.0:

1. Demonstrated low impact on file, database, and application server performance
2. Allowed for more simultaneous VMs than the other solutions tested
3. Consistently outperformed Trend Micro Deep Security 9 and McAfee Move

VMware ESXi 5.5 vShield-Enabled Server Workload Performance

Windows Server 2008 R2 CIFS File Server Performance

as reported by Load DynamiX Test Development Environment 3.2



Note: A nested 72.4GB file set was used for read transactions. Client load emulated by Load DynamiX TDE 3.2, requesting approximately 9:1 read/write transactions. Tests run for a period of 1 hour. Lower impact from baseline is better. Baseline read throughput 43.77MB/s, write throughput, 4.9MB/s.

Source: Tolly, February 2014

Figure 1

The central task of an AV solution is to scan data to detect and block threats. Ideally, the AV solution should impact application performance as little as possible. To evaluate the performance impact of the three solutions, Tolly engineers benchmarked common server and VDI environments. First, tests were run on unprotected systems to establish a performance baseline. Then, each solution was installed and tested. Results measured the performance impact of each solution versus the baseline with lower impact being a better result.

File Server Performance

A Microsoft Windows 2008 R2 server, configured to provide Common Internet File Services (CIFS) sharing, was driven by a load generator that issued reads/writes across the network. The Sophos solution impact on performance was dramatically lower than the other two solutions.

For read transactions, impact on performance for the other solutions was over 4X that of Sophos. For write transactions, the difference in performance was much greater with Trend Micro at over 10X and McAfee at over 15X the impact of Sophos. See Figure 1.

Web Server Performance

The second component of the enterprise workload dealt with performance of the Magento eCommerce web application, simulating a large web retail portal.

Sophos produced the least impact of any solution at 13.25% lower throughput than baseline performance. By comparison, Trend Micro slowed the server response time by an additional 52%, while McAfee's impact was 72% more than Sophos.

Sophos Ltd.

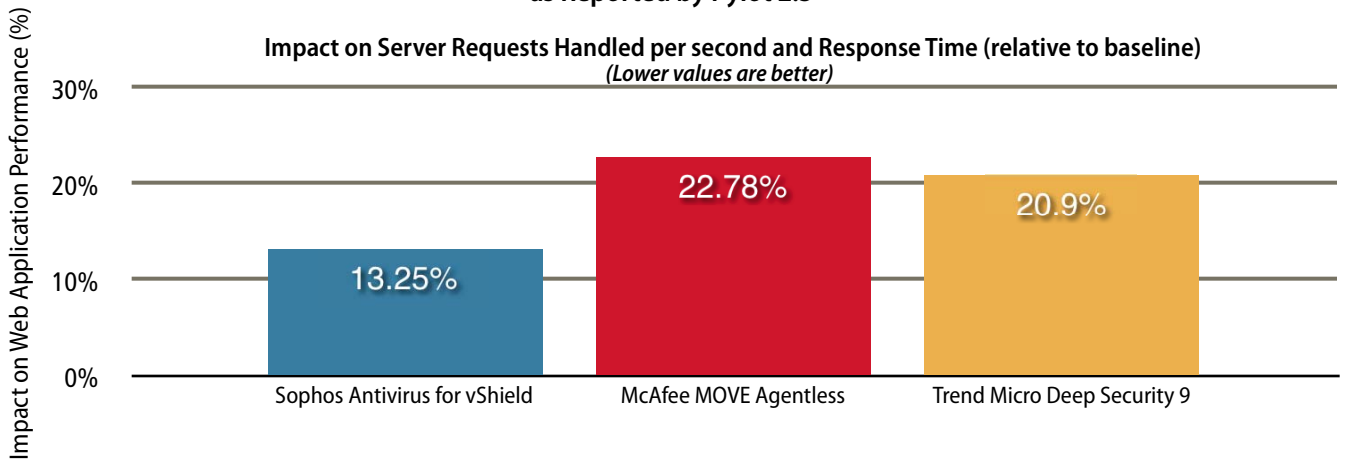
Sophos Antivirus for vShield 1.0

Database, File, and Web Application Server & VDI Performance

Tolly. Certified

Tested February 2014

VMware ESXi 5.5 vShield-Enabled Server Workload Performance
Throughput and Response Time Impact Running Magento eCommerce Web Application
as Reported by Pylot 2.5



Note: Microsoft Server 2008 R2 Install with MySQL 5.1 Database, PHP Zend Server front-end. Pylot configured to emulate 20 clients, concurrently requesting a set of 10 URLs. Test traffic driven by Ubuntu 12.04 LTS 64-bit VM. Tests were run for a period of 1 hour. Results are from a single test, thus impact from baseline is identical for both graphs. Lower impact from baseline is better. Baseline data, Throughput: 5.99 Rps, 3.346 Second response time.

Source: Tolly, February 2014

Figure 2

SQL Database Performance

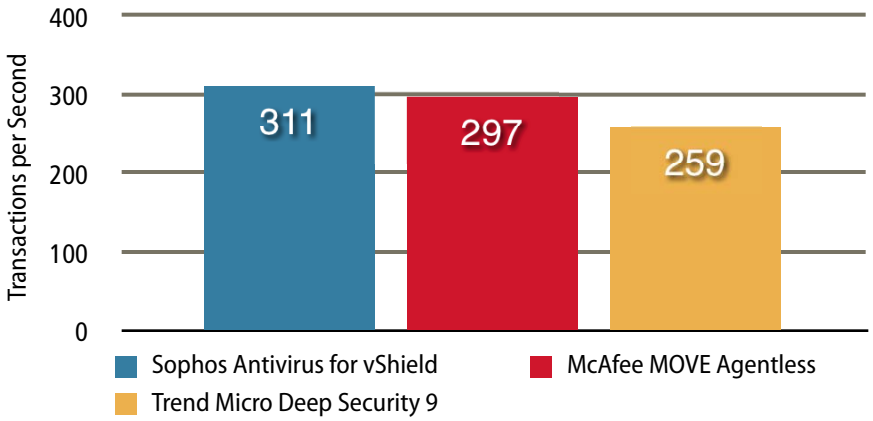
Lastly, engineers constructed a Microsoft SQL Server 2008 database, emulating large-scale order processing. Sophos was able to provide an aggregate 311 transactions per second, 4.7% more than McAfee, and 20% more than Trend Micro in similar configurations.

VDI Performance

To simulate the impact of each solution on a typical VDI environment, Tolly engineers deployed 120 Windows 7 virtual machines on one ESXi 5.5 host, running VMware's View Planner 2.1 workload for a period of 10 hours.

Over the simulated "work day" Tolly measured the aggregate user experience

VMware ESXi 5.5 vShield-Enabled Server Performance
SQL Server 2008 SPEC TPC-C 16 Warehouses, 20 Clients
(as reported by OLTPBench)

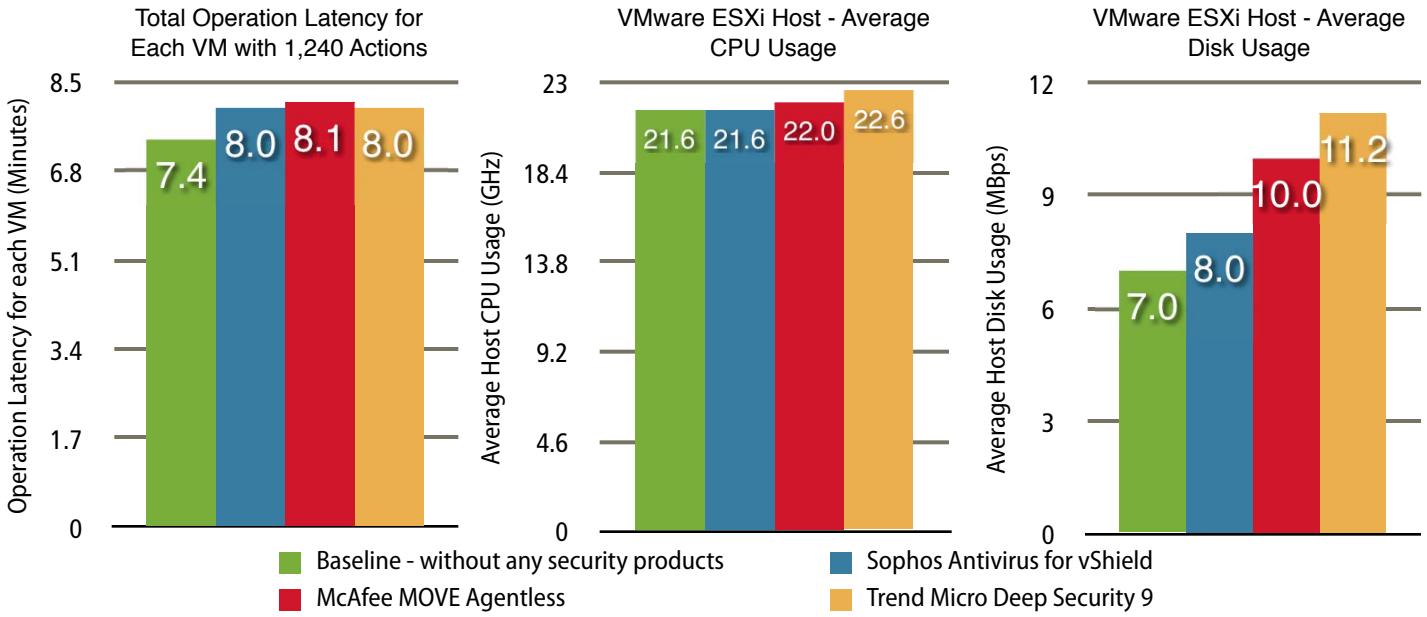


Note: At McAfee's recommendation, SQL Server data files were omitted from real-time scanning. 1.75GB Database size. No exceptions were made for Sophos or Trend Micro.

Source: Tolly, February 2014

Figure 3

VDI Performance Results with the VMware View Planner User Workload
120 Windows 7 Virtual Machines on One Host
(as reported by VMware View Planner 2.1 and vCenter 5.5)
Lower numbers are better.



Notes: Seven iterations of the VMware View Planner 2.1 standard workload with Microsoft Word, Excel, powerPoint, Internet Explorer, Outlook, Media Player, Adobe Reader, Firefox and 7-zip applications were run. For each VM, there were 1,240 operations (e.g. Word open, PPTx-RunSlideShow, outlook-Attachment-Save, etc.).

Source: Tolly, February 2014

Figure 4

delay for each VM, as well as critical metrics from each host. Tolly found that the Sophos solution imposes minimal operation delays on the test system (~7.5%) and is on par with the other vShield solutions.

However, Sophos provides this same user experience while consuming fewer host resources. Measuring the average CPU utilization over the duration of the tests, engineers found that Sophos did not produce a noticeable impact on server CPU resources compared to the baseline, while Trend Micro and McAfee required an additional 1.9% and 4.6% of CPU resources. While relatively small, in sufficiently large environments, this could lead to additional hardware requirements to support the same number of VMs as Sophos.

Similarly, Sophos required less total disk I/O activity than competing solutions for on-access scanning. Over the entire test duration, Sophos averaged 8.0 MBps of disk I/O, while Trend Micro and McAfee consumed 25% and 40% more, respectively.

Test Setup & Methodology

Test Environment

The test environment consisted of two similarly-equipped VMware ESXi 5.5 hosts, each with 2x Intel Xeon X5680 processors (Hex-core, 3.33GHz). Both hosts were equipped with 144GB RAM, 3x 256GB SSDs, and a dual-port 4G FC HBA.

Two HP MSA 2012FC storage arrays were utilized for testing. An array consisting of 12x 450GB 15K RPM drives was used to host the 120 VDI clients, while a 2TB LUN on an array with 12x 1TB 7.2K RPM drives was used for file server storage.

Server Environment

The server environment consisted of three separate application servers, each provisioned from a Microsoft Windows Server 2008 R2 Enterprise base image, equipped with 2vCPUs and 4GB RAM.

One Microsoft SQL Server 2008 instance was used to host the SPEC TPC-C database application. A second server was configured with mySQL 5.5 and Zend Server 6.3 to support the Magento Community Edition eCommerce web application, version 1.8.1.0. A third server was provisioned with Microsoft file services, and acted as a file server, driven by one Load DynamiX 1G storage traffic generator. See Figure 5.

An Ubuntu 12.04 LTS client was loaded with the OLTPBench test application and Pylot 2.5, which was used to load the initial databases and generate requests to the database and web application servers upon execution.

The database server was loaded with a 16-warehouse, SPEC TPC-C-compliant database. The file server was configured with 10 shares, each with 25,000 unique 640KB files, under 5 nested folders, totaling ~100GB of data.

A snapshot of each VM was created to serve as a common starting point for all tests.

VDI Environment

120 Windows 7 Enterprise 64-bit virtual machines were hosted as linked clones on one server with 2x Intel Xeon X5680 processors (Hex-core, 3.33GHz) and 144GB RAM using VMware ESXi 5.5.0. All 120 VMs were stored on one HP MSA 2012FC storage arrays with 12x 450GB 15K RPM drives in RAID 10. The security virtual appliance from each vendor was stored in the same volume and host as all virtual desktops.

Test Execution

For the server environment, tests were run concurrently on all three VMs for a period of one hour. Each server was loaded with the equivalent of twenty work clients.

For the database testing, the OLTPBench application was invoked to emulate 20 database clients performing transactions with the following distribution:

- New Order: 45%
- Payment: 43%
- Order Status: 4%
- Delivery: 4%
- Stock Level: 4%

Transaction counts were collected every two seconds over the duration of the workload.

For the Magento eCommerce web application workload, engineers configured Pylot 2.5 on the Ubuntu test client to request a set of 10 URLs from the Magento web application. These queries consisted of: four product queries, three product categories, the shopping cart, a search by tag, and the main index page.

The requests were load balanced across twenty emulated "agents", which performed requests and response validation. All requests made over HTTP.

For the file server throughput tests, engineers configured the Load DynamiX 1G appliance via the TDE 3.2 with two load profiles, one each for read/write operations, each with 10 emulated clients. The read scenario iterated through the static file server content, while the write scenario

wrote unique data to a separate share, attempting to replicate the initial directory structure. Test configured to have approximately 90% read, 10% write.

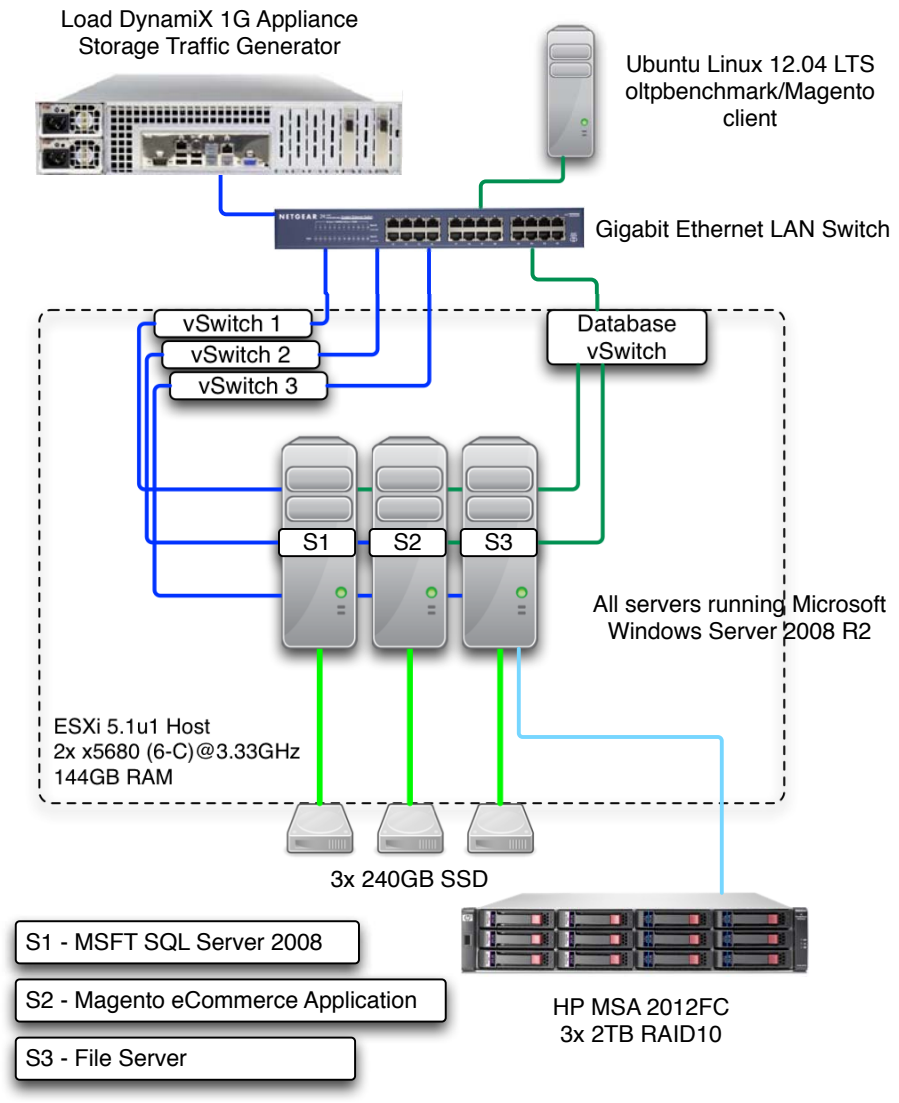
VDI Test with View Planner

The VDI tests were run with 120 VMs to evaluate the user experience and resource consumption. Each VM was running the same VMware View Planner 2.1 standard workload with Microsoft Word, Excel, PowerPoint, Internet Explorer, Outlook, Media Player, Adobe Reader, Firefox and 7-zip applications. Iterations - 7, think time - 20, ramp up time - 600, test type - local were used as the View Planner configuration.

On access scan for each solution under test was enabled. No update or on demand scan was scheduled to run during the test.

All solutions under the test passed the View Planner test. The recorded latency to execute all 1,240 operations on each VM was reported along with the average host CPU and disk usage during the 10 hours test.

Server Test Environment



Note: Elements inside dashes indicate virtual devices.

Source: Tolly, February 2014

Figure 5

Solutions Under Test

Sophos Antivirus for vShield 1.0	
Sophos Enterprise Console	5.2.1.197
Sophos Antivirus for vShield Virtual Appliance	Antivirus version 9.5.1
McAfee MOVE AntiVirus [Agentless] 3.0	
McAfee ePolicy Orchestrator	5.0.1 (Build: 228)
McAfee MOVE AV [Agentless] extension	3.0.0.173
McAfee MOVE AntiVirus [Agentless] on the security virtual appliance	3.0.0.163
Trend Micro Deep Security 9	
Trend Micro Deep Security Manager	9.0.5370
Trend Micro Deep Security Virtual Appliance	9.0.0.2009
Trend Micro Deep Security Filter Driver	9.0.0.995

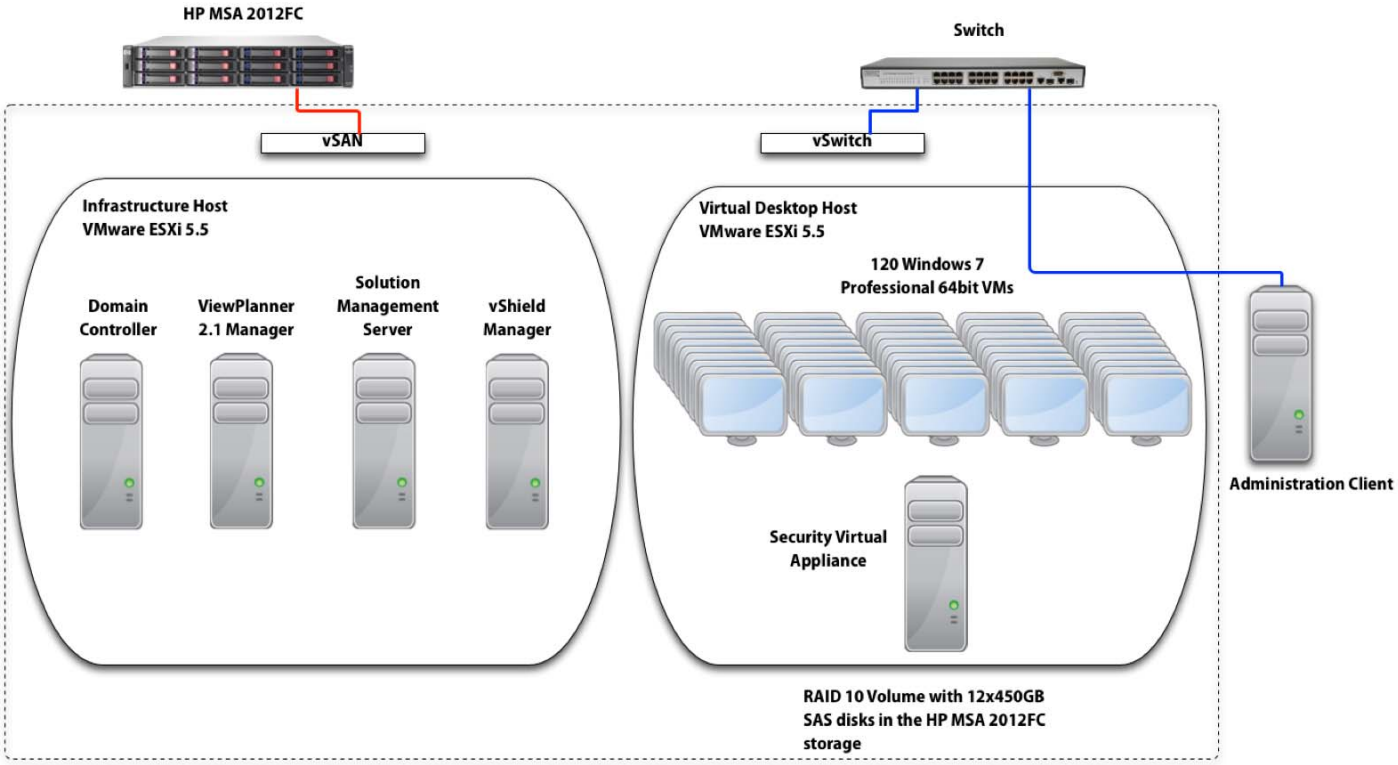
Source: Tolly, February 2014 Table 1

Test Environment

VMware vCenter Server	5.5.0, 1476327
VMware ESXi	5.5.0, 1331820
VMware vShield Manager	5.5.0a-1473628
VMware vShield Endpoint	5.1.0-01255202

Source: Tolly, February 2014 Table 2

VDI Test Environment



Source: Tolly, February 2014

Figure 6

Test Equipment Summary

The Tolly Group gratefully acknowledges the providers of test equipment/software used in this project.

Vendor	Product	Web
Load DynamiX	**Load DynamiX 1G Storage Test Tool**	LOAD DYNAMIX http://www.LoadDynamiX.com

About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 25 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by E-mail at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at: http://www.tolly.com

Interaction with Competitors

In accordance with Tolly's Fair Testing Charter, Tolly personnel invited representatives from Trend Micro, Inc. and McAfee to participate in the testing. Trend Micro did not reply, while McAfee offered configuration guidance and was provided with its results prior to publication.

For more information on the Tolly Fair Testing Charter, visit:

http://www.tolly.com/FTC.aspx

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is," and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

214110 TP-2 YX-JT-2014-04-04-Verl