

Endpoint Security Solutions (Physical & VDI Environment)

Comparative Testing Analysis



VENDORS TESTED:

McAfee | Sophos | Symantec | Trend Micro

EXECUTIVE SUMMARY

Indusface was commissioned by Trend Micro Inc. to carry out a series of independent performance evaluations through comparative tests on the industry's best competitive endpoint security solutions in both physical and virtual environments. The testing was conducted from December 2011 to January 2012 following industry-standard best practices for client configuration and test-case design.

This independent testing of Trend Micro OfficeScan against leading enterprise endpoint security solutions was undertaken to help ascertain that OfficeScan continues to be the fastest and most efficient endpoint security solution*. With threat protection through the Smart Protection Network's unique file and web reputation capabilities, and optional integrated Data Loss Protection, Trend Micro OfficeScan is the only solution to offer a combination of performance and effectiveness that organizations large and small require to protect their data and users from threats.

PRODUCTS & VERSIONS

Objective performance testing was conducted on the following enterprise endpoint protection security software products on Windows 7 Ultimate Edition.

- Trend Micro Office Scan (OSCE) 10.6
- McAfee VirusScan Enterprise (MFE) 8.8
- Symantec Endpoint Protection (SEP) 12.1
- Sophos Endpoint Security and Control (SESC) 9.7

Comparative performance testing was conducted on a subset of enterprise endpoint security products in a Virtual Desktop Infrastructure (VDI) configuration. The products in VDI testing were the latest available at the time of testing and included the following:

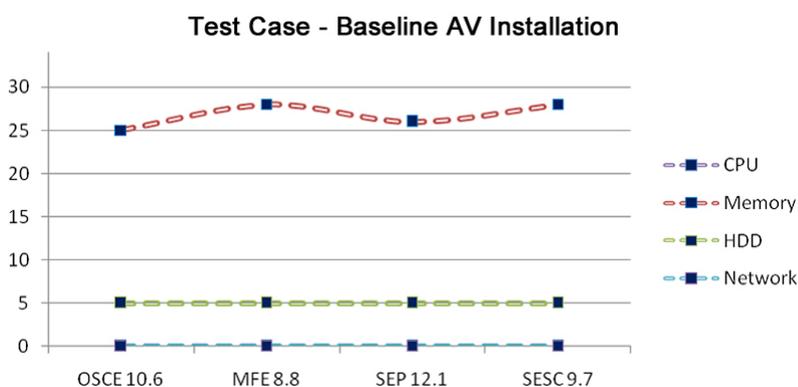
- OfficeScan 10.6 with VDI Plug-In
- McAfee MOVE 2.0 for VDI
- Symantec Endpoint Protection 12.1

TEST RESULTS – PHYSICAL CLIENTS

The descriptions below highlight test cases and results from testing of physical clients.

TEST CASE – BASELINE AV INSTALLATION

Approach: Systems memory, HDD, network & CPU data are recorded after the installation of the endpoint agent.



Result: It was observed that Trend Micro OfficeScan 10.6 utilizes the lowest endpoint resource after AV installation on the endpoint system. This observation proves that endpoint resources are available for more end user activity with OfficeScan 10.6, consuming 4-11% less memory than competitors products.

Reference Note: * Comparative Analysis on Endpoint Security Solutions 2010

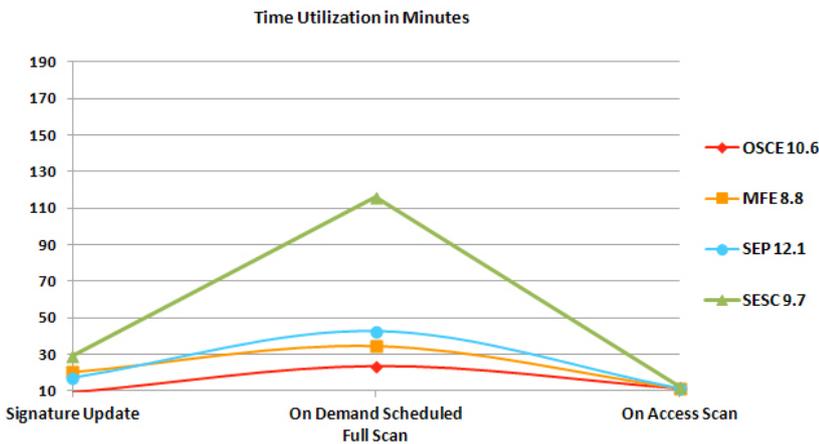
TEST CASE – SIGNATURE UPDATE

Approach: Scheduled updates were turned off for three days after the installation of the end point manager server. After three days, the updates are collected and are pushed from the server to the endpoint clients. Respective resource utilizations were recorded during the signature update.

Result: Trend Micro OfficeScan 10.6 completed the client update in nearly 50% of the time required by the nearest competitor, Symantec Endpoint Protection 12.1. Trend Micro OfficeScan significantly outperforms the competitors in this test case, and the difference compared to other products is a result of Smart Scan powered by Trend Micro Smart Protection Network, which off-loads a large number of signatures that were previously stored on endpoint computers to smart protection sources.

TEST CASE – ON DEMAND SCHEDULED FULL SCAN

Approach: After the endpoint client installation, a scan is run on all endpoints in order to build caches for clients that use some form of scan results caching; resource utilization of this cache-building scan is not recorded. For the recorded test, an on-demand full scan (equivalent to the most common kind of scheduled scan in customer environments) was executed and resource utilization of CPU, memory and disk utilization on the endpoint client was recorded for the full scan initiated from the server

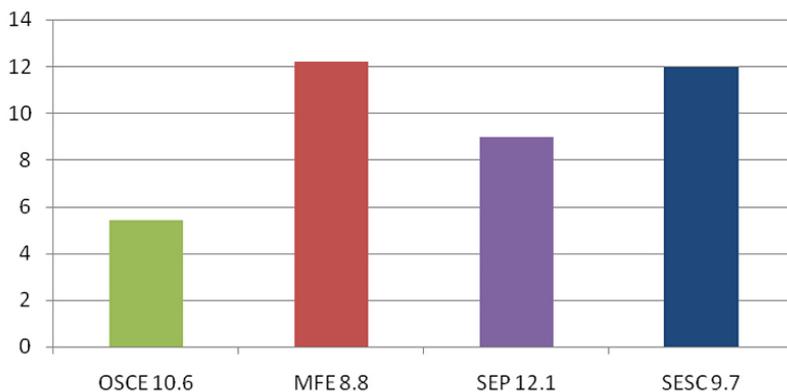


scan in customer environments) was executed and resource utilization of CPU, memory and disk utilization on the endpoint client was recorded for the full scan initiated from the server

Result: Trend Micro OfficeScan 10.6 was 33% and 45% faster than McAfee and Symantec products, respectively. The chart at left compares the time (in minutes) needed by the tested products to complete a scheduled scan.

TEST CASE – ON ACCESS SCAN

Approach: Different types of data files of size 2 GB were copied on the endpoint client from a network file server, and resource utilization was recorded for the time of completion of data copy. This test case was executed five times and the average resource utilization was calculated.



Result: While there was little variation for On-Access scans across tested products when measuring time taken, and network, disk and memory usage, in the area of CPU

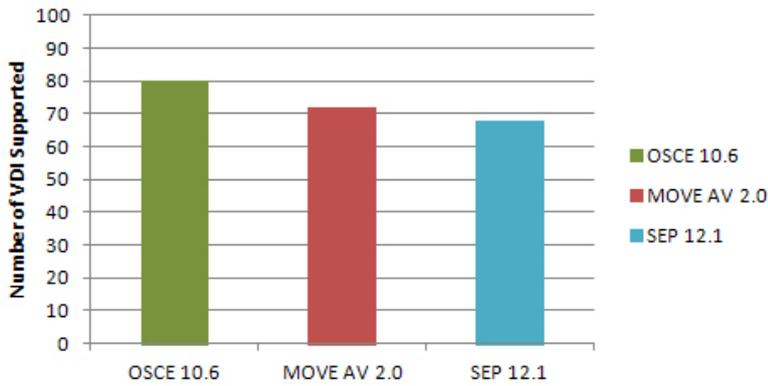
utilization OfficeScan used significantly less CPU resources (5.4%) compared to 9% by Symantec Endpoint Protection and 12.2% by McAfee VirusScan.

TEST RESULTS – VDI TESTING

Several test cases were run against OfficeScan and competitor products in a VDI environment.

Number of VDI Comparison

A test was conducted to determine the maximum number of VDI clients (agent-based) that the product



could support before an observable decrease in server performance. The VDI infrastructure was assessed on Dell Power Edge R900 4 * 2.93 GHz Quad Core Xeon Processor with 64 GB of Memory and 2 TB of Hard disk on RAID. The number of VDI’s supported is calculated based on the server response after the installation of AV and with light workload on the endpoints. Workload was simulated

using scripts with multiple applications in order to provide a consistent benchmark for the simulated end-user activity.

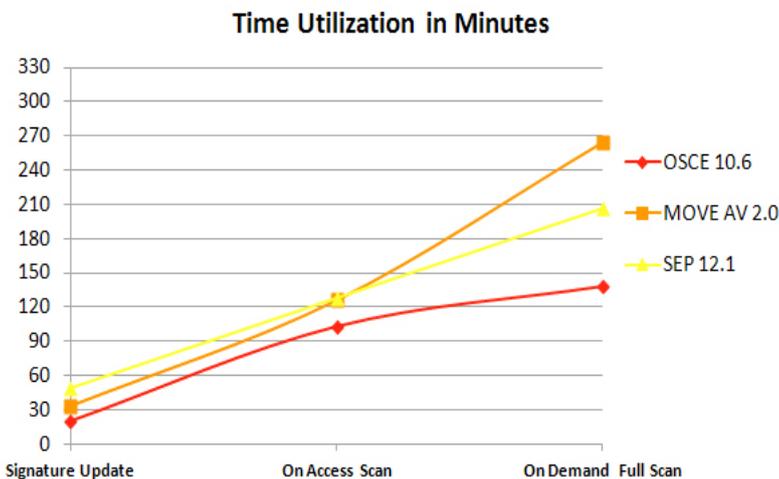
The standalone tests for CPU, memory and disk utilization demonstrated that OfficeScan was able to achieve 10-15% higher consolidation than Symantec and McAfee solutions through more efficient use of system resources during both idle and scan times.

TEST CASE – BASELINE AV INSTALLATION

Approach: The systems memory, HDD, network & CPU data is recorded for ESX Server after the installation of AV on all the VDI’s.

Result: Trend Micro OfficeScan 10.6 utilized 10-16% less CPU and memory resource after the in-guest endpoint agent installation on the endpoint systems. As a result endpoint resources are available for more end user activity with OfficeScan 10.6.

TEST CASE – SIGNATURE UPDATES



Approach: Scheduled updates were turned off for three days after the installation of the endpoint manager server. After three days, the updates are collected to server and are pushed from server to all of the VDI clients. Respective resource utilizations were recorded during the signature update for the ESX Server.

Test Case – On Demand Full Scan

Approach: An On Demand Full Scan was initiated on the all the VDI Clients.

Resource utilization (CPU, memory, hard disk and network) and time taken for On Demand Full Scan was recorded for the ESX Server.

TEST CASE – ON ACCESS SCAN

Approach: Different types of data files of size 500 MB were copied on all the VDI clients from the network file server. Resource utilization was recorded for the duration of the time needed to complete the data copy.

Results: For signature updates, On Demand Full Scans, and On-Access (real-time) scans, the OfficeScan in-guest VDI client performed significantly faster than endpoint security solutions from Symantec and McAfee. The graph above illustrates the performance differences between OfficeScan 10.6 and the tested competitors, measured by the time taken to complete the tested action for all 60 VDI clients.

CONCLUSION

Based on meticulous testing using industry-standard configurations and test cases, Indusface concludes that Trend Micro OfficeScan 10.6 continues to deliver best-in-class performance in physical and virtual client environments when objectively compared to enterprise endpoint protection solutions from Symantec, McAfee and Sophos. Organizations of all sizes can deploy Trend Micro to their endpoints with confidence that they are taking advantage of the industry's best performing endpoint security agent.



www.trendmicro.com

About Trend Micro

Trend Micro is a global leader with more than 20 years of expertise in endpoint, messaging and web security. Trend Micro is focused on innovating smarter security solutions that protect against a wide range of insidious threats and combined attacks including viruses, spam, phishing, spyware, botnets, and other web attacks, including data-stealing malware. Trend Micro's is the next generation cloud-client content security infrastructure, which beats conventional methods by combining Internet-based technologies with smaller, lighter weight clients to stop threats before they reach users.



www.indusface.com

About Indusface

Indusface is a privately-held, award winning, innovative, visionary, fast growing security company, trusted by fortune 500 organizations across the globe. Indusface caters to more than 400 satisfied customers worldwide from various industry verticals and enjoys global security partnerships. Indusface is a Deloitte Technology Fast 50 India, Nasscom Emerge 50 and Red Herring Top 100 Asia award winning organization.

APPENDIX: FEATURE COMPARISON MATRIX

Features	Trend Micro Office Scan 10.6	McAfee Virus Scan Enterprise	Symantec Endpoint Protection 12.1	Sophos Endpoint Security and Control 9.7
Protection Point				
Desktops, Laptops, Servers	✓	✓	✓	✓
Operating Systems	✓	✓	✓	✓
Protection Type				
Detects and removes conventional threats (viruses, spyware, root kits and bots)	✓	✓	✓	✓
Phishing and Content Filtering	✓	✓	✓	✓
Protects Online Transactions	✓	✓	✓	✓
Locks down select files and folders (e.g. Intuit QuickBooks)	✓	✓	✓	✓
Device Control	✓	✓	✓	✓
Scan Cache	✓	✓	✓	✗
Cleanup Services	✓	✓	✓	✓
Advanced Protection				
Firewall	✓	✓	✓	✓
Data Loss Prevention	✓	✗	✗	✓
In the Cloud Protection	✓	✗	✓	✗
ISD/IPS	✓	✗	✓	✗
Zero Day Attack Protection	✓	✓	✓	✓
Restricting Potentially Unwanted Programs	✓	✓	✓	✓
Management				
Central Management Console	✓	✓	✓	✓
Configuring alerts and notifications	✓	✓	✓	✓
Scanning				
Full Scan	✓	✓	✓	✓
Real Time Scan	✓	✓	✓	✓
Smart Scan	✓	✗	✗	✗