

Symantec Corporation

Symantec Endpoint Protection 11.0.3

Evaluación del rendimiento competitivo en

comparación con Kaspersky, McAfee y Trend Micro en Windows XP



Resumen
de la prueba

Premisa: La minimización del impacto del rendimiento de las soluciones de seguridad en los tiempos de respuesta de computadoras host, aumenta la aceptación por parte del usuario de los programas de seguridad y disminuye el deseo de deshabilitar dichos programas. Al instalar una solución de bajo impacto, las organizaciones podrán posponer inversiones en hardware para nuevos clientes y lograr paralelamente una mejor experiencia del usuario.

Symantec Corporation solicitó a The Tolly Group que evaluara el impacto de las ofertas de seguridad en los puntos extremos de clase empresarial en la capacidad de respuesta de los clientes del mercado computacional.

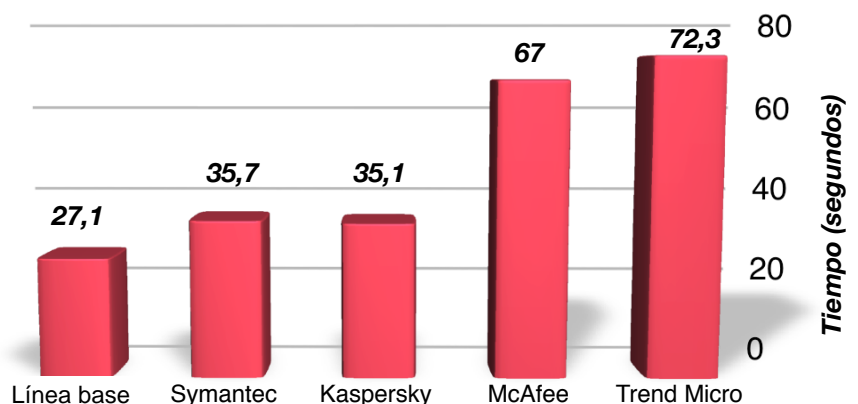
The Tolly Group comparó la versión de cliente de Symantec Endpoint Protection 11.0.3 para Windows XP, la cual cuenta con funcionalidad de antivirus, contra programas espía, cortafuegos, prevención de intrusión en el host y control de aplicaciones y dispositivos, todo en un único agente con las ofertas de seguridad de Kaspersky Lab, McAfee, Inc. y Trend Micro, Inc. (Consulte la Figura 8 para conocer una lista detallada de los productos que se probaron).

The Tolly Group analizó el tiempo de inicio del sistema, el impacto en Microsoft Office 2007, en Internet Explorer, en el manejo de archivos y en el tiempo necesario para descomprimir un fichero. Las pruebas se realizaron en octubre de 2008.

Aspectos destacados de la prueba

- ▶ Una computadora con Symantec Endpoint Protection se inició dos veces más rápido que una computadora con Trend Micro OfficeScan y 88% más rápido que un sistema con McAfee Total Protection for Endpoint
- ▶ Symantec fue el único proveedor que no disminuyó la velocidad de apertura de archivos de Microsoft Word y de presentaciones en PowerPoint, mientras que McAfee duplicó el tiempo necesario para abrir un documento de Word de 1,2 MB
- ▶ El impacto de Symantec al iniciar Internet Explorer fue menor que el 10%, mientras que Kaspersky, McAfee, Trend Micro disminuyeron la velocidad del sistema en más del 50%

Tiempo de inicio desde la pantalla del logotipo de Windows XP hasta un estado "inactivo"



Las barras más bajas son lo mejor

Nota: El tiempo de inicio se midió desde la pantalla de logotipo de Windows XP hasta que la CPU del host pasó a estado inactivo. Resultados redondeados a una décima de segundo.

Fuente: The Tolly Group, octubre de 2008

Figura 1

Resumen ejecutivo

Symantec Endpoint Protection 11.0.3 proporcionó constantemente tiempos de respuesta más rápidos que los productos probados de la competencia. En el mejor de los casos, Symantec Endpoint Protection 11.0.3 alcanzó tiempos de respuesta dos veces más rápidos que algunos productos probados de la competencia.

Las soluciones de Endpoint Security están diseñadas para inspeccionar y analizar cada archivo que se abra o escriba en el disco duro. El motor del antivirus analiza el archivo y lo compara con su depósito de virus conocidos, a fin de garantizar que no haya ningún contenido malicioso ni ninguna secuencia de comandos dañina en el mismo. Esta operación puede tener un impacto no trivial en el rendimiento de aplicaciones como Microsoft Word y PowerPoint, o en otros procesos normales de la computadora.

En los sistemas con Symantec Endpoint Protection 11.0.3, los documentos de Word y las presentaciones de PowerPoint se abrieron más rápido que en los sistemas con Kaspersky

Tiempo de inicio de Windows XP desde el logotipo de Windows hasta el estado inactivo

Proveedor	Producto	Tiempo promedio de inicio (segundos)	Delta de tiempo a la línea base (porcentaje)
Línea base	Sólo sistema operativo	27,09	0
Kaspersky Lab	Work Space Security	35,05	29%
McAfee	Total Protection for Endpoint	67,04	147%
Symantec	Symantec Endpoint Protection 11.0.3	35,68	32%
Trend Micro	OfficeScan 8.0	72,27	167%

Fuente: The Tolly Group, octubre de 2008

Figura 2

Tiempos de respuesta asociados a la apertura de un archivo de Word de 1,2 MB en una computadora con Windows XP

Proveedor	Producto	Tiempo promedio en que se abre un archivo (segundos)	Delta de tiempo a la línea base (porcentaje)
Línea base	Sólo sistema operativo	3,74	0
Kaspersky Lab	Work Space Security	4,8	28%
McAfee	Total Protection for Endpoint	7,29	95%
Symantec	Symantec Endpoint Protection 11.0.3	3,63	-3%
Trend Micro	OfficeScan 8.0	4,97	33%

Fuente: The Tolly Group, octubre de 2008

Figura 3

Work Space Security, McAfee Total Protection for Endpoint o Trend Micro OfficeScan.

Los ingenieros de The Tolly Group probaron los productos en seis escenarios de tiempo de respuesta:

- Tiempo de inicio desde la pantalla del logotipo de Windows hasta un estado “inactivo”
- Abertura de un documento de Word de 1,2 MB
- Tiempo para abrir una presentación de PowerPoint
- Tiempo necesario para ejecutar Internet Explorer y abrir una página Web
- Tiempo para copiar y pegar un archivo de texto de 1 GB
- Tiempo para descomprimir un fichero de 1 GB

Las pruebas muestran que Symantec Endpoint Protection 11.0.3 brinda tiempos de respuesta más rápidos que otros productos probados de manera regular, normalmente haciendo un paralelo con los tiempos de respuesta que brinda una prueba de línea base, al ejecutar la operación sin ningún software de seguridad.

RESULTADOS

TIEMPO DE INICIO

El rapido tiempo de arranque en los teléfonos

inteligentes mantiene a los usuarios cada vez más insatisfechos con los largos tiempos de inicio en las computadoras; es por esto que fabricantes como Dell e Intel invierten bastante dinero en tecnologías para acelerar los procesos de inicio. Por otra parte, muchas aplicaciones de seguridad prolongan el tiempo de inicio. Las pruebas muestran que Symantec Endpoint Protection agregó sólo 8,6 segundos al proceso de inicio.

Esta prueba midió el tiempo que demora iniciar una máquina desde el logotipo inicial de Windows hasta que el proceso de inactividad del sistema se estabiliza en 99% durante 10 segundos. Esto indica que todos los servicios se han cargado y que la computadora responde al ingreso del usuario.

Las pruebas línea base, fueron ejecutadas en un sistema operativo Windows XP SP3 sin aplicacion de seguridad. El sistema logró iniciarse en 27,1 segundos. Consulte la Figura 2.

La computadora con Symantec Endpoint Protection se inició en 35,7 segundos, dos veces más rápido que el sistema con Trend Micro OfficeScan (72,3 segundos) y 88% más rápido que el sistema con McAfee Total Protection for Endpoint (67 segundos).

Symantec Endpoint Protection 11.0.3 estuvo a la par con Kaspersky Work Space Security (35,1 segundos).

MICROSOFT WORD

Microsoft Word es la aplicación de Office más popular y un software de seguridad no debiera interferir significativamente en

Symantec Corporation
Endpoint Protection
11.0.3



Impacto del tiempo de respuesta de sistemas de seguridad en los puntos extremos, en computadoras con el cliente Windows XP

Especificaciones del producto

La información proporcionada por el proveedor no está necesariamente verificada por The Tolly Group

Symantec Endpoint Protection 11.0.3

Beneficios:

- Symantec Endpoint Protection combina Symantec AntiVirus con una avanzada prevención contra amenazas, a fin de brindar defensa sin igual contra programas maliciosos en computadoras portátiles, de escritorio y servidores. Integra sin problemas tecnologías de seguridad fundamentales en un único agente y consola de administración, aumentando la protección y ayudando a reducir el costo total de propiedad.
- Mejor calidad de experiencia del usuario final, mediante el uso eficaz de los recursos del sistema.

Características:

- Integra sin problemas tecnologías fundamentales, tales como antivirus, contra programas espía, cortafuegos, prevención de intrusión y control de dispositivos y aplicaciones.
- Necesita solamente un único agente, el cual es controlado por una consola de administración única.
- Brinda protección inigualable en los puntos extremos del del líder en el mercado de seguridad de puntos extremos.
- Habilita la actualización instantánea de Network Access Control (NAC) sin el despliegue de software adicional para cada punto extremo.
- Optimiza el uso de espacio y recursos del cliente para adaptarse a todos los entornos comerciales.

Symantec Corporation

20330 Stevens Creek Blvd.
Cupertino, CA 95014
URL: www.symantec.com

su rendimiento al abrir un documento. Los ingenieros midieron el tiempo necesario para abrir un documento de Word de 1,2 MB hasta que estuvo listo para editarse.

Las pruebas muestran que Symantec Endpoint Protection no redujo la velocidad de esta operación. Microsoft Word pudo abrir el documento en 3,6 segundos en un sistema con Symantec Endpoint Protection 11.0.3 instalado o dos veces más rápido que con McAfee Total Protection for Endpoint (7,3 segundos). Consulte la Figura 3.

Kaspersky Work Space Security requirió 4,8 segundos, McAfee Total Protection usó 7,3 segundos y Trend Micro requirió 5,0 segundos para realizar la misma operación.

MICROSOFT POWERPOINT

Generalmente, las presentaciones de PowerPoint son más grandes que los documentos de Word. Los ingenieros de The Tolly Group eligieron una presentación de diapositivas de 10 MB y realizaron una prueba similar a la del documento de Word.

La solución de McAfee nuevamente tuvo el impacto adverso más alto, agregando dos segundos a la operación; le siguió

Tiempos de respuesta asociados a la abertura de un archivo de PowerPoint de 10 MB en una computadora con Windows XP

Proveedor	Producto	Tiempo promedio en que se abre un archivo (segundos)	Delta de tiempo a la línea base (porcentaje)
Línea base	Sólo sistema operativo	4,18	0
Kaspersky Lab	Work Space Security	5,41	29%
McAfee	Total Protection for Endpoint	6,34	52%
Symantec	Endpoint Protection 11.0.3	4,04	-3%
Trend Micro	OfficeScan 8.0	4,69	12%

Fuente: The Tolly Group, octubre de 2008

Figura 4

Tiempos de respuesta relacionados con el inicio de Internet Explorer en una computadora con Windows XP

Proveedor	Producto	Tiempo promedio en que se abre un archivo (segundos)	Delta de tiempo a la línea base (porcentaje)
Línea base	Sólo sistema operativo	3,39	0
Kaspersky Lab	Work Space Security	5,31	57%
McAfee	Total Protection for Endpoint	6,49	91%
Symantec	Endpoint Protection 11.0.3	3,74	10%
Trend Micro	OfficeScan 8.0	5,62	66%

Fuente: The Tolly Group, octubre de 2008

Figura 5

Kaspersky con 1,2 segundos. Trend Micro agregó solamente un segundo al proceso, mientras que Symantec estuvo a la par con el tiempo de la base línea. (Consulte la Figura 4.)

Kaspersky Workspace requirió 5,4 segundos, McAfee Total Protection usó 6,3 segundos y Trend Micro requirió 4,7 segundos para realizar la misma operación.

INTERNET EXPLORER

Esta prueba midió la capacidad de respuesta de Internet Explorer durante la ejecución y el tiempo necesario para cargar un sitio Web, como Yahoo y Reuters. Debido a que la velocidad de la red depende del rendimiento externo, se configuró un servidor interno para imitar el sitio de muestra, de modo que se estableciera un rendimiento bien definido.

Las pruebas indican que la línea base, sin un software de seguridad, cargó Internet Explorer en sólo 3,4 segundos.

Symantec Endpoint Protection 11.0.3 se ubicó justo detrás de esa cifra, con 3,7 segundos, o dentro del 10% del tiempo de línea base, lo que representa así el producto de mayor velocidad de la prueba. Los otros productos que se prueban mostraron tiempos de carga de Internet Explorer con rangos que oscilaron entre

Tiempos de respuesta de una operación de copiar/pegar con un archivo de 1 GB en una computadora con Windows XP.

Proveedor	Producto	Tiempo promedio en que se abre un archivo (segundos)	Delta de tiempo a la línea base (porcentaje)
Línea base	Sólo sistema operativo	43,9	0
Kaspersky Lab	Work Space Security	46,01	5%
McAfee	Total Protection for Endpoint	45,84	4%
Symantec	Endpoint Protection 11.0.3	44,54	1%
Trend Micro	OfficeScan 8.0	44,88	2%

Fuente: The Tolly Group, octubre de 2008

Figura 6

Tiempo para descomprimir un fichero que contenga un archivo de texto de 1 GB en una computadora con Windows XP

Proveedor	Producto	Tiempo promedio en que se abre un archivo (segundos)	Delta de tiempo a la línea base (porcentaje)
Línea base	Sólo sistema operativo	339,39	0
Kaspersky Lab	Work Space Security	614,89	81%
McAfee	Total Protection for Endpoint	879,25	159%
Symantec	Endpoint Protection 11.0.3	422,03	24%
Trend Micro	OfficeScan 8.0	601,36	77%

Fuente: The Tolly Group, octubre de 2008

Figura 7

57% y 91% más lentos que el resultado de línea base. (Consulte la Figura 5.)

COPIA DE ARCHIVOS

Las aplicaciones de seguridad con funciones de protección automática, como las que se probaron, reducen invariablemente la velocidad de manejo de archivos. La minimización del impacto debe ser el objetivo de todo proveedor de seguridad.

Los ingenieros de The Tolly Group midieron la cantidad de tiempo requerido para copiar y pegar un archivo de texto de 1 GB. Una vez más, el sistema con Symantec Endpoint Protection mostró el menor impacto al prolongar el proceso en 0,64 segundos (44,54 segundos en comparación con la línea base de 43,9 segundos).

El impacto de Kaspersky Work Space y McAfee Total Protection fue hasta un 400% superior que el impacto que produjo Symantec. El impacto del segundo producto de mayor velocidad, Trend Micro OfficeScan, fue aún un 100% superior que Symantec Endpoint Protection.

DESCOMPRESIÓN DE FICHEROS

Las aplicaciones de seguridad analizan los ficheros a medida que éstos se descomprimen. Esta medición registró el tiempo requerido para

descomprimir un conjunto de archivos comprimidos desde un fichero. Estas medidas cedieron el tiempo requerido para descomprimir una colección de documentos comprimidos en un archivo.

La línea base para descomprimir el archivo de texto de 1 GB fue de 339,4 segundos. Symantec Endpoint Protection 11.0.3 realizó la tarea en 24% de dicho tiempo, en 422 segundos. Una vez más, la solución de seguridad de Symantec registró el mejor rendimiento de todos los productos que se probaron.

Trend Micro OfficeScan requirió 601,4 segundos para realizar la tarea, Kaspersky Work Space Security requirió 614,9 segundos y McAfee Total Protection utilizó 879,3 segundos. (Consulte la Figura 7.)

METODOLOGÍA Y CONFIGURACIÓN DE LA PRUEBA

Los ingenieros de The Tolly Group ejecutaron todas las pruebas en sistemas idénticos configurados con un procesador Intel Pentium 4 3.4 GHz, 2GB de RAM y un disco duro de 160GB corriendo a 7,200 RPM

Cada aplicación de seguridad se instaló con la configuración predeterminada, pero se configuró para comparar de forma precisa todas las otras aplicaciones de seguridad durante las pruebas de comparación de la misma categoría (es decir, todas las aplicaciones tuvieron habilitadas las funciones de protección automática contra amenazas.)

Después de la instalación y actualización, el tiempo se distribuyó en procesar cualquier perfil requerido, configuraciones del sistema o de caché en segundo plano, según lo requerido por la aplicación. Se realizaron reinicios después de cada prueba.

El banco de pruebas consistió en sistemas computacionales idénticos, todos configurados con la misma imagen fantasma de Microsoft Windows XP SP 3 y Microsoft Office 2007 Professional. Se utilizó otra computadora conectada a la red aislada para mostrar las imágenes de XP y de software en prueba (SUT, por sus siglas en inglés) en cada computadora. Se agregó una clave al registro, la cual habilitó el inicio de sesión automático como el administrador local.

Se crearon seis escenarios de prueba para evaluar el rendimiento de Symantec Endpoint Protection 11.0.3 en comparación con los software comparables de protección en los puntos extremos de otros importantes proveedores. Las pruebas incluyeron lo siguiente:

- Tiempo de inicio desde la pantalla del logotipo de Windows hasta un estado “inactivo”
- Abertura de un documento de Word de 1,2 MB
- Tiempo para abrir una presentación de PowerPoint
- Tiempo necesario para ejecutar Internet Explorer y abrir una página Web

⌚ Tiempo para copiar y pegar un archivo de texto de 1 GB

⌚ Tiempo para descomprimir un fichero de 1 GB

METODOLOGÍA DE TIEMPO DE INICIO

Una secuencia de comandos AutoIt registró el tiempo al comienzo del proceso de inicio, cuando el equipo mostró la pantalla del logotipo inicial de Windows y el tiempo cuando el proceso de inactividad del sistema se estabilizó en 99%.

Después de registrar los tiempos en un archivo de registro, se reinició la computadora y se ejecutó la secuencia de comandos para tres iteraciones.

METODOLOGÍA DE INTERNET EXPLORER

Se escribió y ejecutó una secuencia de comandos AutoIt para cada computadora. Al hacer doble clic sobre el icono de Internet Explorer, la secuencia de comandos comenzó a registrar el tiempo que la computadora requirió para iniciar el explorador y navegar a una página Web en un servidor HTTP.

Los ingenieros crearon un servidor Web Apache en la red local. Estos mismos copiaron en el servidor algunas páginas Web estáticas de sitios Web comerciales. La secuencia de comandos indicó a los usuarios que abrieran las páginas Web en el servidor local. Luego que la página

Web se cargó completamente, la secuencia de comandos registró el tiempo en un archivo de registro, la computadora se reinició y ejecutó la secuencia de comandos para tres iteraciones.

METODOLOGÍA DE MICROSOFT WORD

Se escribió y ejecutó una secuencia de comandos AutoIt para cada computadora. Al hacer doble clic en un icono de documento de Word, la secuencia de comandos comenzó a registrar el tiempo que tardó la computadora en abrir el documento de Microsoft Word y finalizó el registro cuando éste se cargó por completo. La secuencia de comandos registró el tiempo en un archivo de registro, se reinició la computadora y se ejecutó la secuencia de comandos para tres iteraciones. Se agregó una secuencia de comandos al registro, la cual habilitó el inicio de sesión automático como el administrador local.

METODOLOGÍA DE MICROSOFT POWERPOINT

Se escribió y ejecutó una secuencia de comandos AutoIt para cada computadora. Al hacer doble clic en un icono de documento de PowerPoint, la secuencia de comandos comenzó a registrar el tiempo que tardó la computadora en abrir la presentación de PowerPoint y finalizó el registro cuando ésta se cargó por completo.

Después que el documento se cargó completamente, la secuencia de comandos registró el tiempo en un archivo de registro, se reinició la computadora y se ejecutó la secuencia de comandos para tres iteraciones.

METODOLOGÍA DE COPIA DE ARCHIVO

Se escribió y ejecutó una secuencia de comandos AutoIt

para cada computadora. Al hacer doble clic con el botón derecho del mouse sobre un icono de un documento de texto de 1 GB y copiarlo, la secuencia de comandos comenzó a registrar el tiempo que tardó la computadora en copiar el documento y luego pegarlo en un subdirectorio diferente. La secuencia de comandos finalizó el registro cuando se copió el archivo en su destino y desapareció el cuadro de diálogo de copia de archivo. La secuencia de comandos registró el tiempo en un archivo de registro, se reinició la computadora y se ejecutó la secuencia de comandos para tres iteraciones.

METODOLOGÍA DE DESCOMPRESIÓN DE FICHEROS

Se escribió y ejecutó una secuencia de comandos AutoIt para cada computadora. Los ingenieros hicieron doble clic con el botón derecho del mouse sobre el icono de un archivo de texto de 1 GB en un fichero con 20,000 archivos y seleccionaron la opción "Extraer". Esto, a su vez, inició una secuencia de comandos que registró el tiempo que demoró la computadora en descomprimir los contenidos del documento comprimido y finalizó el registro cuando se descomprimió completamente en una carpeta en el escritorio.

HERRAMIENTAS UTILIZADAS

El tiempo delta % calcula el porcentaje de tiempo de la Línea Base que representa la solución protegida y es calculada restando la Línea Base por el tiempo de protección, dividiendo el número por la línea base y multiplicando por 100. Por ejemplo cuando una ejecución protegida toma 35.1 segundos contra una línea base de 27.1 la diferencia es de 8 segundos o 29.5% de la ejecución de la Línea Base.

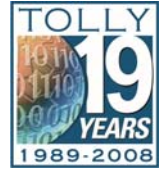
Productos probados y versiones de software

Proveedor	Producto	Versión
Kaspersky Lab	Work Space Security	6.0.3.837
McAfee	Total Protection for Endpoint	8.7.0
Symantec	Endpoint Protection	11.0.3
Trend Micro	OfficeScan	8.0 Build 1004

Fuente: The Tolly Group, octubre de 2008

Figura 8

The Tolly Group es un proveedor líder mundial de servicios de validación para proveedores de productos, componentes y servicios TI.



La empresa tiene su casa matriz en Boca Raton, FL y se puede acceder a ella comunicándose al teléfono +1 (561) 391-5610 o mediante Internet en:
 Sitio Web: <http://www.tolly.com>,
 Correo electrónico: sales@tolly.com

Fair Testing Charter™
 Interacción con la competencia

The Tolly Group no consideró necesario comunicarse con el proveedor de la competencia, debido a que los productos están diseñados para que los usuarios puedan instalarlos sin asistencia.



Términos de uso

USE ESTE DOCUMENTO SÓLO SI ACEPTA ESTOS TÉRMINOS.

Este documento se proporciona de forma gratuita, para ayudarle a comprender si un producto, una tecnología o un servicio merecen un análisis más profundo según sus necesidades específicas. Cualquier decisión de compra se debe realizar a partir de su propia evaluación de idoneidad.

Esta evaluación se concentró en ilustrar las funciones específicas o el rendimiento de los productos y se llevó a cabo en condiciones controladas de laboratorio, y algunas pruebas pueden haberse adaptado para reflejar el rendimiento en condiciones ideales; el rendimiento puede variar en condiciones reales. Los usuarios deben realizar pruebas a partir de sus propios escenarios reales para validar el rendimiento en sus propias redes. Se hicieron los esfuerzos comercialmente pertinentes para garantizar la precisión de los datos presentados aquí, pero cabe la posibilidad de que existan errores o descuidos. Bajo ningún caso The Tolly Group será responsable de daños de cualquier naturaleza, incluso daños directos, indirectos, especiales, contingentes y emergentes que puedan derivarse del uso de la información contenida en este documento.

La prueba/auditoría documentada aquí puede, también, depender de varias herramientas de prueba cuya precisión está fuera de nuestro control. Además, el documento utiliza ciertas afirmaciones del patrocinador, cuya verificación va más allá de nuestro control. Entre dichas afirmaciones está el hecho de que el software/hardware probado se produzca o existan planes para su producción, y de que el software/hardware probado está o estará disponible en una forma equivalente o mejor para los clientes comerciales.

Cuando existan traducciones a otro idioma, el documento en inglés se debe considerar como el documento autorizado. Para garantizar la precisión, use solamente los documentos descargados directamente desde el sitio Web de The Tolly Group. Todas las marcas comerciales son propiedad de sus respectivos titulares.

208349-tbnvfm4-cdb-19NOV08