



NOD 32

Expert Antivirus System

Cada tanto, el mundo de la tecnología nos sorprende con la aparición una “*killer application*”, es decir, una solución innovadora que convierten en obsoleto todo lo hasta ahora conocido. **NOD32**, desarrollado por la firma Eset, reúne todas las características para ser una “*killer application*” de los actuales antivirus pues no solo brinda una insuperable protección contra virus conocidos y desconocidos, sino que también permite olvidarse de pesados antivirus que lentifican el funcionamiento de los equipos, mejorando la performance de las PCs sin añadir hardware.- La innovadora filosofía de trabajo de **NOD32** es obra del Dr. Anton Zajac, quien en los años 90 fue nominado como candidato a recibir el Premio Nobel de Física.- El Dr. Zajac es el actual presidente y CEO de Eset.-

Los antivirus tradicionales (Ej. Norton, McAfee, Trend, etc.) trabajan fundamentalmente en base a “firmas” de virus. Cada vez que examinan un archivo, hacen una comparación contra el archivo “firmas” y de coincidir informan que se trata de un virus.-

Lo anterior tiene varios inconvenientes, alguno de los cuales son:

- trabajan de manera “reactiva”, primero aparece el virus y luego la solución, por lo que no brindan ningún tipo de defensa contra nuevos virus.-
- son muy fáciles de engañar mediante simples tretas que utilizan los virus.-
- dado que cada día hay más virus, el archivo de “firmas” ve incrementada diariamente su dimensión, y su procesamiento y el método de comparación consumen grandes recursos de los equipos, originando quejas de los usuarios.

NOD32 en cambio reconoce los virus de manera más inteligente, instalando en la PC un experto virtual que, utilizando diversas herramientas, efectúa un análisis de los códigos de los archivos, estudiando su comportamiento, apoyado en una base de conocimientos que contiene los comportamientos típicos de los virus. Es decir, **NOD32** utiliza recursos propios de la inteligencia artificial.-(1)

Esta técnica, conocida como “heurística de los antivirus” no es nueva, e incluso algunos de los antivirus tradicionales dicen utilizarla, si bien lo hacen de una manera muy insuficiente comparada con la de **NOD32**. En general se la había descartado por su lentitud y por los errores que producía, usualmente conocidos como “falsos positivos” y “falsos negativos”, limitaciones estas que la tecnología de Eset ha superado, logrando resultados asombrosos como los que se exponen en la hoja adjunta.

Algunas características destacadas de **NOD32**:

- Un record sin precedentes en la detección de **virus conocidos**. Desde Mayo de 1998 **NOD32** ha detectado todos los virus “In the Wild” (3), hazaña nunca lograda por ningún otro antivirus. Esto surge de los informes de Virus Bulletin, rigurosa auditora inglesa especializada en el control de calidad de antivirus.-
- Protección contra **virus desconocidos**. La innovadora tecnología heurística de **NOD32** ha permitido la detección de nuevos virus, aún desconocidos en su momento, como por ejemplo Melissa, FunLove, Kriz, Happytime, CIH, y cientos de nuevas infecciones, sin que haya sido necesario ningún tipo de actualización especial del sistema antivirus.-
- **NOD32** ha demostrado constantemente ser entre **2 y 50 veces más rápido** en el análisis de archivos ejecutables que cualquier otro programa antivirus.-

- **NOD32** necesita entre **2 y 20 veces menos recursos de sistema** que otros antivirus.- Con lo que las aplicaciones en general corren más rápidamente, sin necesidad de modificar el hardware. Sugerimos la lectura del estudio (4) que Canon (Japón) realizara sobre este tema. Canon, eligió NOD32 para uso interno, y por las sobresalientes capacidades que encontró en él, también optó por traducirlo al japonés y vendérselo a sus clientes. Actualmente Canon es uno de los mayores distribuidores de NOD32.-
- Además de las clásicas revisiones “on-access” a cargo de AMON (Antivirus Monitor) y “on-demand”, **NOD32** cuenta con un segundo módulo de revisión, el IMON (Internet Monitor) que revisa todo el tráfico de Internet y DMON especial para documentos de Office.
- De sencilla integración con otras herramientas. Por ejemplo, utilizado conjuntamente con componentes “free” tales como Mail Scanner y Spam Assassin, sobre plataforma Linux, es posible lograr una protección integral del correo corporativo, a nivel de gateway, que protege contra virus (con múltiples antivirus), spam y filtrado de contenidos, solución esta de muy alto rendimiento, a un costo menor en casi un 90% a otras soluciones (ej. la de Trend, Symantec, Surf Control, Mail Sweeper, etc), las que, no obstante sus mayores costos, no ofrecen la totalidad de las prestaciones que la integración descrita brinda.-

NOD32 corre sobre plataformas Intel y compatibles, estando disponible para ambientes operativos Windows 9x, 2000, 2003 y XP, DOS, Unix, Linux, Netware, Lotus Notes, MS Exchange, etc. con versiones especiales para Dell NAS y Kerio (Proxy-Firewall y Mail Server), contando con recursos de administración centralizada para soportar complejas redes corporativas.-

El servicio de soporte provee servicio de instalación “llave en mano”, que incluye la desinstalación del antivirus que se este utilizando.-

Eset cuenta con oficinas en USA y Europa, y distribuidores de NOD32 en más de 100 países. Información adicional puede obtenerse en www.nod32-a.com

QUE DICEN LOS ESPECIALISTAS SOBRE **NOD32**

NOD 32 es el único de 17 productos evaluados que ha detectado el 100% de todas las muestras infectadas a través de todos los conjuntos de pruebas, tanto de análisis de scanner como en las pruebas de interceptación en tiempo real (monitor) y sin emitir un solo falso positivo. NOD32 también ha establecido un nuevo record en la tasa de velocidad de revisión de disco duro.

La mejor detección, mayor velocidad, mayor rendimiento

VIRUS BULLETIN (2)

NOD32 es hoy en día, el antivirus más rápido y eficiente del mercado, habiendo ganado 21 premios (5) consecutivos de Virus Bulletin 100%, la prestigiosa publicación de la industria antivirus, entre otros 21 productos analizados, por su nivel de detección y limpieza total con un 100% de eficiencia.

Por algo Microsoft lo utiliza en varios equipos de trabajo, incluyendo el grupo de servicio de Lanzamiento de Productos, donde es necesario analizar terabytes de datos y código propietario antes de su liberación pública.

NOD32 posee la capacidad de examinar más de cinco millones de KB por segundo, siendo este resultado, más del doble de velocidad que el mejor producto que le sigue en cualquier comparativa realizada y teniendo además, una exclusiva y avanzada tecnología heurística que provee un excepcional rendimiento en cientos de miles de lugares de trabajo.

VS Antivirus

... que NOD32, un antivirus sin tanto marketing....., haya ganado todos los premios VB 100% desde que se presentó, es un hecho ha tener en cuenta; no tienen mas que probarlo para darse cuenta de la calidad de ese antivirus ... Realmente yo considero a NOD32, muy superior a otros AVs conocidos como Norton, McAfee y PC-Cillin...

Foro Virus Attack!

Si esta cansado del software que que devora espacio en el disco y ciclos del CPU, NOD32 es el producto antivirus para usdes. NOD32... utiliza una sofisticada heurística avanzada que logra características de análisis muy precisas, combinando una perfecta tasa de detección con un rendimiento aun no superado. Eset realizó un excelente trabajo al equilibrar el desempeño y una protección sobresaliente, como lo prueba el éxito continuo de NOD32...

PC MAGAZINE

NOD32 prácticamente no impacta en la performance de las PC. Esa cualidad unida a su insuperable nivel de detección determino que nuestra corporación lo haya adoptado para su utilización interna y para proveerlo a nuestros clientes.-

TOM TAKAMOTO
Digital Security Laboratory
Canon Systems Solutions
Japón

(en www.nod32.com.ar se puede acceder al detalle de los estudios realizados por Canon)

(1)Fuente: Entrevista que realizara Ignacio Sbampato a Richard Marko, ingeniero de Eset, <http://www.encyclopediavirus.com/encyclopedia/articulo.php?id=343>

(2)Fuente: Virus Bulletin, Febrero 2001

(3)Se denomina "In the Wild" a las pruebas efectuadas sobre virus reales, en contraposición a las efectuadas en colecciones de laboratorios.

(4)Informe disponible, en inglés, en www.nod32-a.com

(5)Con posterioridad a estas declaraciones , NOD32 ha ganado varios premios 100 % adicionales a los 21 mencionados.-

COMPARATIVA DE ANTIVIRUS

<u>SOFTWARE</u>	<u>FALLAS</u> (1)	<u>DEGRADACION</u> (2)	<u>TECNOLOGIA</u> (3)
NOD32	0	+ 6 %	proactiva
Symantec	89	+ 491 %	reactiva
McAfee	93	+ 98 %	reactiva
Trend	3.443	+ 33 %	reactiva

- (1) Cantidad de fallas (virus omitidos de detectar) según los tests de la firma auditora inglesa Virus Bulletin (www.virusbtn.com) período 06/02 a 08/04 para Windows y Novell Netware.
- (2) Indica la degradación en la performance que produce la utilización del Antivirus. El estudio fue realizado por Canon – Japon, y esta disponible en www.nod32-a.com
- (3) NOD32 utiliza heurística Standard (análisis de código) y avanzada (ejecución del código en una PC virtual), lo que le permite detectar códigos desconocidos. Los demás productos estan basados en reconocimientos por comparación con códigos de virus conocidos.