



## LANDesk® Host Intrusion Prevention

Añada prevención a la protección

## Mayor protección contra los ataques dirigidos



“Si el malware sigue creciendo al ritmo actual, existe la posibilidad de que los creadores de software antivirus no sean capaces de aguantar el ataque”.

— “¿Están luchando las empresas antivirus en una guerra que no pueden ganar?”, Idm.net.au, citando a Eugene Kaspersky de Kaspersky Labs

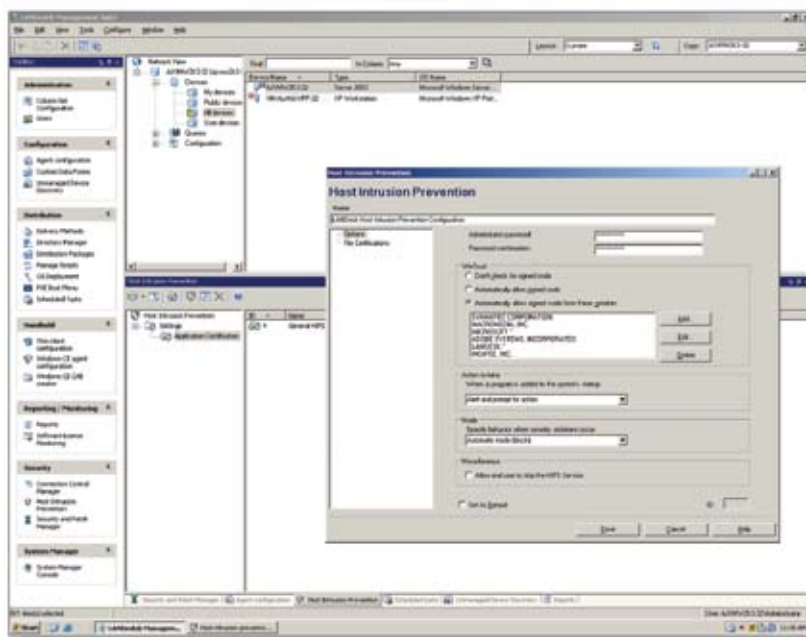
Es una realidad que los piratas informáticos son cada vez más rápidos y enrevesados. Por eso, los métodos tradicionales de proteger los sistemas de la empresa, es decir, software antivirus y servidores de seguridad, ya no son suficientes para garantizar el funcionamiento continuado de los sistemas y que la propiedad intelectual crítica no caiga en las manos equivocadas. Mikko Hypponen, director jefe de investigación de F-Secure, un proveedor de servicios de seguridad, contaba que algunos días recibe nada menos que 40.000 nuevos archivos contaminados para los que se han de crear firmas de antivirus. “Esta batalla no es simplemente entre fabricantes de software de seguridad y algunos criminales de Internet. Es una guerra entre el bien y el mal”, continuaba. (“¿Están luchando las empresas de antivirus en una guerra que no pueden ganar?”, idm.net.au)

Usted puede llevar a cabo su propia guerra y preguntarse en qué momento la próxima amenaza del día cero acabará con toda o parte de su empresa. Puede preguntarse a qué puede hacer frente su servidor de seguridad o solución antivirus. O bien, puede optar por reforzar su entorno de seguridad existente con protección contra ataques dirigidos a nivel de host y proporcionarle a su empresa un nivel de protección incluso mayor.

### LANDesk® Host Intrusion Prevention: Tranquilidad añadida

LANDesk® Host Intrusion Prevention le ayuda a frustrar los ataques malintencionados mediante procedimientos de bloqueo basado en el comportamiento que impiden que las aplicaciones se ejecuten de forma indeseada en un sistema host individual. Y es más, LANDesk Host Intrusion Prevention funciona desde la misma consola que emplea el personal informático para administrar LANDesk® Security Suite y LANDesk® Management Suite. Acceda a todo lo que necesita para la solución de seguridad por capas de LANDesk® más completa disponible, como:

- Mayor seguridad y el conocimiento de estar equipado para impedir las amenazas del día cero incluso antes de que haya una solución disponible.
- Mayor eficacia y menores costes de formación e infraestructura gracias a una única solución de consola que ofrece una completa seguridad por capas.
- Control preciso sobre lo que los usuarios pueden y no pueden hacer en los sistemas de la empresa.



LANDesk® Host Intrusion Prevention frustra los ataques malintencionados gracias a procedimientos de bloqueo basados en el comportamiento que se administran directamente desde la misma consola que se emplea para administrar LANDesk® Security Suite.

## Prevención añadida a la protección desde una única consola

Es esencial que sus sistemas estén actualizados con los parches de las últimas definiciones de antivirus y asegurarse de que los virus conocidos no dañen nunca datos críticos o afecten a la productividad de los usuarios. Pero con el rápido aumento de los ataques del día cero (sólo en 2007 se han producido más de 20 vulnerabilidades del día cero), su empresa podría estar aún en peligro, a pesar de contar con la mejor solución antivirus disponible. Y aquí es donde entra LANDesk® Host Intrusion Prevention. Funciona en combinación con LANDesk® Security Suite y LANDesk® Antivirus desde una sola consola administrativa para proporcionarle una capa de protección añadida, la prevención.

LANDesk Host Intrusion Prevention no sólo protege contra virus conocidos existentes y otros ataques malintencionados, sino que le permite prevenirse contra ellos al supervisar y detener comportamientos sospechosos: los tipos de comportamientos propios de los ataques malintencionados. Incluso si una definición de antivirus no se encuentra aún disponible, puede reforzar su protección contra los ataques. Como tecnología madura que es, LANDesk Host Intrusion Prevention ostenta un impresionante historial al haber bloqueado vulnerabilidades de malware durante más de 10 años, como las similares a Zotob, Storm, Code Red, Nimda y el virus Blaster, incluso antes de que aparecieran firmas de antivirus.

## Control preciso con listas blancas de aplicaciones

Mediante dos métodos distintos, LANDesk® Host Intrusion Prevention permite al personal de TI determinar no sólo aquellas aplicaciones que no se pueden ejecutar, sino también las que sí se pueden. Por una parte, puede utilizar la protección de seguridad estándar de HIPS para impedir automáticamente cualquier comportamiento de software malintencionado. Para un nivel de control aún más personalizado, aplique protección de seguridad basada en listas blancas y ejecute únicamente aquellas aplicaciones que se incluyen en su "lista blanca" o lista de aplicaciones aprobadas. Todas las demás aplicaciones tienen denegada la ejecución.

LANDesk Host Intrusion Prevention permite también al personal de TI determinar las aplicaciones que están autorizadas para enviar correo electrónico, modificar las claves del registro protegidas y escribir en archivos ejecutables y procesos protegidos. El personal de TI está capacitado para impedir que nuevas aplicaciones malintencionadas, ésas que podrían hacerse pasar por las aplicaciones de uso diario, atraviesen las defensas de la empresa. Las amenazas nuevas y emergentes, como vulnerabilidades por desbordamiento del buffer y amenazas del día cero, se pueden supervisar y, además, contener.

## Nine Protection Styles of Host-Based Intrusion Prevention

	Block the Known Bad (Allow All Else)	Allow the Known Good (Block All Else)	Unknown
Behavior-Level HIPS	7 Resource Shielding	8 Application Hardening	9 Behavioral Containment Passive → Active
Application-Level HIPS	4 Antivirus	5 System Hardening	6 Application Inspection
Network-Level HIPS	1 Attack-Facing Network Inspection	2 Personal Firewall	3 Vulnerability- Facing Network Inspection

Source: Gartner (May 2005)

127317-01

LANDesk® Host Intrusion Prevention en combinación con LANDesk® Security Suite y LANDesk® Antivirus le proporcionan prácticamente los nueve estilos de protección de Gartner de la prevención de intrusión basada en host.

## Una solución de seguridad por capas incluso más completa: la simplicidad de una única consola

LANDesk® Host Intrusion Prevention es un complemento de LANDesk® Security Suite. Su uso en combinación con LANDesk Security Suite y LANDesk® Antivirus constituye una solución de seguridad por capas incluso más completa, con un control centralizado aún más amplio sobre todo el entorno de red.

- LANDesk Security Suite lleva la administración activa de la seguridad hasta los puntos finales. Ofrece funciones de cuarentena, análisis activo de las amenazas, detección y eliminación de spyware, control de acceso, herramientas de seguridad de la configuración y mucho más.
- LANDesk Antivirus proporciona protección contra los virus empresariales y detección de programas invasores rootkit desde la simplicidad de una única consola que sólo se encuentra en las soluciones de LANDesk®. Permite aplicar la mejor protección antivirus a toda la empresa por una inversión mucho menor que la requerida por otras soluciones estándar del sector.

LANDesk Host Intrusion Prevention utiliza y amplía la potencia de LANDesk Security Suite y LANDesk Antivirus para proporcionarle una solución de seguridad más completa (también se puede utilizar con LANDesk Security Suite y otros productos antivirus destacados del sector).

# Características principales

## Control desde una única consola

- Permite a los administradores de TI utilizar una sola consola de administración para instalar, configurar y administrar funciones de prevención de intrusión basada en host en todos los sistemas de la empresa.
- Permite al personal de TI perpetuar rápida y fácilmente los comportamientos aprendidos bloqueados en un host individual en los sistemas host de toda la empresa.

## Protección del sistema de archivos y el registro

- Reconoce las modificaciones malintencionadas realizadas en el registro para impedir la ejecución de malware cuando se reinicia un sistema host.
- Permite al personal de TI bloquear el registro hasta que el administrador de TI apruebe las modificaciones.
- Permite a los administradores de TI impedir que ciertas clases de malware ejecuten funciones malintencionadas en el sistema de archivos al especificar qué procesos tienen prohibidas qué operaciones y en qué archivos.
  - Procesos: pueden ser “todos” los procesos o algunos procesos designados.
  - Operaciones: puede ser “ninguna” operación o determinadas operaciones predefinidas (lectura, escritura, ejecución, creación).
  - Archivos: pueden ser “todos” los archivos o nombres de archivo predefinidos, incluyendo comodines. Por ejemplo: “FILE.ABC”, “\*.EXE” etc.
  - Según las reglas mencionadas anteriormente y las certificaciones de los procesos solicitantes, el resultado es “permitir” o “denegar” la operación.

## Control de inicio del sistema

- Facilita a los administradores de TI un proceso para la creación de una lista blanca de aplicaciones que se pueden ejecutar al iniciarse el host, junto con una lista negra de otras que no se pueden ejecutar.
- Ofrece a los administradores de TI un control preciso sobre las aplicaciones que se pueden ejecutar en los sistemas de la empresa y cómo se permite la ejecución de tales aplicaciones.
- Proporciona protección añadida contra los ataques malintencionados al impedir que aplicaciones malintencionadas disfrazadas nuevas y/o desconocidas traspasen las defensas de la empresa.
- Proporciona configuraciones flexibles para diferentes perfiles de usuario de modo que diferentes usuarios y grupos tengan diferentes listas blancas.

## Control de programas invasores rootkit y del acceso a las aplicaciones

- Permite al personal de TI determinar si las aplicaciones en funcionamiento pueden ejecutar otras aplicaciones en un host con el fin de detectar e impedir que programas invasores o rootkits se infiltren sigilosamente en los sistemas de la empresa.
- El filtro de red a nivel del núcleo permite al personal de TI definir los archivos ejecutables de una aplicación, así como lo que es y no es un comportamiento aceptable de la red.
  - El personal de TI puede filtrar la red y bloquear las aplicaciones que intenten conectarse a servidores de correo SMTP salvo que tengan autorización explícita para enviar correo electrónico.
- Proporciona al personal de TI el control sobre qué aplicaciones pueden leer, escribir o modificar archivos o partes del registro protegidos.
  - Al bloquear los cambios en el registro, impide que se inicie el malware en la memoria y/o que se efectúen cambios en el registro.
- Crea un registro con los programas invasores malintencionados no certificados, que se puede perpetuar en toda la empresa.

## Certificación de procesos y archivos

- Capacita a los administradores de TI para certificar que determinadas aplicaciones o archivos puedan omitir algunas o todas las protecciones integradas en LANDesk® Host Intrusion Prevention.
  - Se puede conceder a los usuarios el derecho para modificar los archivos protegidos.
- Impide que los procesos no certificados se mezclen con los certificados y obtengan de forma ilegal atributos de autorización certificados.

## Visite [www.landesk.com](http://www.landesk.com) para más información

Esta información se ofrece en relación con los productos de LANDesk®. Este documento no concede ninguna licencia ni garantía, explícita o implícita, por desestimación o de otro tipo. LANDesk no garantiza que este material esté libre de errores. Además, se reserva el derecho a actualizarlo, corregirlo o modificarlo, incluidas las especificaciones y las descripciones de productos, en cualquier momento y sin aviso previo. Si desea consultar la información más actualizada sobre productos, visite <http://www.landesk.com>.

Copyright © 2007 LANDesk Software, Ltd. o sus filiales. Reservados todos los derechos. LANDesk es una marca registrada o marca comercial de LANDesk Software, Ltd. o sus filiales en Estados Unidos u otros países. Otros nombres o marcas pueden reclamarse como propiedad de otros. Los resultados de cada cliente pueden variar dependiendo de los hechos y circunstancias exclusivos de cada caso.