



LANDesk® Antivirus

Máxima sencillez y protección antivirus en el ámbito de la empresa

Protección de sistemas de toda la empresa desde una sola consola

Todas las empresas tienen la imperiosa necesidad de proteger sus datos y de mantener en perfecto funcionamiento sus sistemas de punto final. Pero el pago, la instalación, la administración y la formación en diferentes productos para garantizar la seguridad de punto final, así como la administración de parches, la protección antivirus y la administración de sistemas pueden repercutir sobre el balance final, ponen a prueba la paciencia del personal de TI y la capacidad a largo plazo de la empresa para prosperar y superar a la competencia.

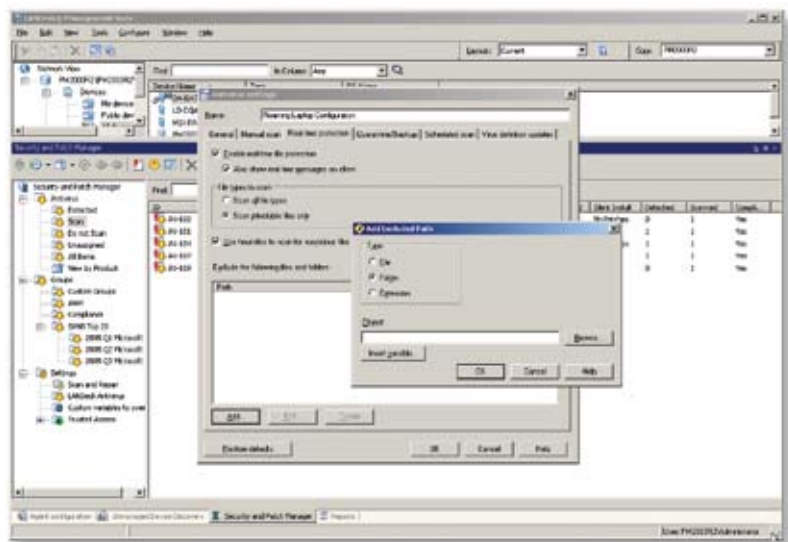
El retraso entre la publicación de parches y la explotación de las vulnerabilidades de los puntos finales sigue un rápido descenso. En el año 2003, el virus Blaster atacó 28 días después de que se descubriera la vulnerabilidad que le permitía actuar. Eso es tiempo más que suficiente para instalar un parche, si se actúa de forma activa y dinámica. Pero a finales de 2005, el ataque a las vulnerabilidades de Msddds.dll y WMF se produjo antes de que hubiera parches disponibles. La amenaza del día cero se está convirtiendo cada vez más en una realidad. Si bien la administración de parches sigue teniendo una importancia crucial, se requiere una protección antivirus activa y dinámica que garantice la seguridad de la red ante cualquier ataque. est indispensable pour sécuriser votre réseau contre les attaques.

LANDesk® Antivirus: la protección antivirus en el ámbito de la empresa combinada con la sencillez del control desde una sola consola

LANDesk® Antivirus amplía la capacidad de LANDesk® Management Suite y LANDesk® Security Suite para ofrecer una solución empresarial antivirus que, además, detecta programas invasores rootkit, todo desde una misma consola y del mismo proveedor al que confía la administración de seguridad y de sistemas, con una inversión más baja que muchas soluciones de la competencia. En definitiva, para aplicar la mejor protección antivirus a los puntos finales, no necesitará realizar grandes desembolsos, ni nuevas infraestructuras, ni gastos de formación, ni nuevos proveedores, y no tendrá que afrontar nuevos problemas. Podrá disponer de administración y protección completa desde una sola consola.

LANDesk Antivirus ayuda a:

- Aplicar la mejor protección antivirus a toda la empresa por una inversión mucho menor que la requerida por otras soluciones de la competencia.
- Reducir costes y complejidad con una solución de protección antivirus y de detección de programas invasores *rootkit* de terceros en el ámbito de la empresa mediante un solo agente y una sola consola.
- Proteger datos vitales para la empresa así como la productividad de los usuarios mediante la identificación, la reducción y la atenuación en tiempo real del riesgo que puede suponer la propagación de virus.
- Dar al personal de TI control absoluto para adecuar la configuración antivirus a las normativas de la empresa e impedir la intervención y los errores de los usuarios finales.
- Ahorrar tiempo y liberar recursos con una solución centralizada, automatizada y sin intervención para detectar y atenuar los efectos de los virus y su propagación en sistemas administrados por soluciones LANDesk®.
- Dotar al personal de TI y a los ejecutivos de una forma rápida y fácil de ver qué sistemas están protegidos o son vulnerables y cómo evoluciona la protección antivirus.



LANDesk® Antivirus ayuda a implementar una protección antivirus en tiempo real.

Características principales

La mejor detección y protección antivirus

- Disponga de las mejores funciones antivirus en el ámbito de la empresa e implemente una protección antivirus en tiempo real.
- Controle las actualizaciones de motores y de archivos de definiciones con detecciones planificadas de sistemas de destino, funciones de detección inmediata para emergencias, etc.
- Prepare la implementación de actualizaciones de archivos de definiciones en un grupo de ordenadores piloto o de prueba durante el tiempo que quiera antes de realizar la instalación distribuida del archivo en toda la organización.
- Permita que los usuarios inicien detecciones, pero conserve el control centralizado para impedir que anulen las detecciones automáticas.
- Utilice menos espacio en los equipos de usuario con recursos de archivos pequeños y discretos que puedan detectar rápidamente vulnerabilidades, malware y virus.
- Detecte vulnerabilidades en datos adjuntos a mensajes de correo de Outlook

Centralización de la configuración y de la administración

- Bloquee el agente de usuario final para impedir cambios no autorizados.
- Use administración según tipo de usuarios para otorgar privilegios para añadir, eliminar o cambiar opciones de configuración LANDesk® Antivirus, central y cliente.
- Adecue la administración antivirus a las normativas de la empresa, con control total y ampliable sobre quién puede implementar el agente, a qué dispositivos y cómo se configura para cada uno de esos dispositivos.

Validación e implementación de archivos de definiciones de virus de la manera más fácil

- Implemente nuevos archivos de definiciones de virus de forma rápida y selectiva en un grupo piloto, mientras pospone la implementación en el resto de la red hasta que se hayan validado los archivos.
- Defina fácilmente los miembros del grupo piloto como parte de la configuración y automatice la correcta distribución de los archivos para cada instalación distribuida.
- Realice la instalación distribuida de archivos de definiciones de virus por fases y minimice el riesgo de que uno de los nuevos archivos implementados provoque efectos inesperados en los recursos o los usuarios de la red.
- Planifique actualizaciones automáticas de los archivos de definiciones de virus y controle qué versiones se aprueban, cuándo se implementan y cómo se configuran.
- Conceda a los usuarios finales la posibilidad de iniciar actualizaciones de antivirus, en caso necesario, pero mantenga el control sobre si pueden acceder únicamente a las actualizaciones aprobadas por TI o si pueden acceder a las actualizaciones en línea directamente desde LANDesk®.
- Regrese a archivos de definiciones de virus anteriores si alguno de los archivos nuevos provoca problemas.

Cuarentena de archivos

- Cifre y ponga en cuarentena archivos sospechosos e infecciones conocidas que no puedan limpiarse al instante.
- Ofrezca la posibilidad de disponer de acceso opcional exclusivamente para ver la carpeta de cuarentena, de tal manera que los usuarios puedan ver lo que contiene pero que no puedan abrir un archivo sospechoso con los riesgos de infección que ello comportaría.
- Detecte automáticamente archivos en cuarentena cuando se publiquen nuevas definiciones de virus y devuelva los archivos que se hayan limpiado correctamente al uso activo.
- Realice copias de seguridad automáticas de los archivos limpiados por si se dañaran archivos que requirieran reparaciones adicionales.
- Personalice su solución para detectar, atrapar y atenuar posibles virus. Opte en cada caso por un control metódico y minucioso o por un control automático rápido y sin intervención.

Informes y alertas

- Reciba alertas por correo electrónico, buscapersonas o el método de su elección cuando no sea posible limpiar automáticamente un equipo.
- Ejerza un control minucioso de todos los detalles de las alertas relativas a las acciones de cuarentena y limpie cualquier contenido sospechoso.
- Cree consultas e informes personalizados que combinen datos de inventario con información de antivirus y de configuración.
- Identifique ordenadores infectados, en los que no se hayan realizado recientemente detecciones en busca de virus o que tengan archivos de definiciones de virus desfasados.
- Proporcione a los usuarios finales notificaciones sobre los procesos de detección y de eliminación de virus.
- Genere informes de actividades e historial de antivirus para saber qué recursos son vulnerables y qué virus se detectan.
- Use los informes de LANDesk® Antivirus para identificar y atenuar los riesgos, así como para instruir a los usuarios sobre las actividades que pueden provocar infecciones.

LANDesk® Executive Dashboard

- Acceda a un simple panel gráfico para identificar propagaciones de virus en tiempo real, así como para disponer de gráficas temporales de actividades de control de virus.
- Demuestre fácilmente al personal ejecutivo los progresos y la importancia crucial del departamento de TI.
- Sepa al instante el porcentaje de ordenadores con definiciones de virus actualizadas y con la función de antivirus en tiempo real activada.

Ejecución obligatoria de soluciones antivirus de terceros

- Administre soluciones de McAfee, Norton, Sophos, Symantec y Trend-Micro mediante la misma consola.

Visite 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 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.

LSI-0677SP 1107/BB/KL