

www.hauri-la.com

Enjoy your Internet with Perfect Security

Qué es el motor ViRobot?

El motor ViRobot es famoso por su alto rendimiento en diagnóstico y reparación. También incluye una poderosa característica que permite manejar incluso virus desconocidos operando en diferentes tipos de plataformas. El motor ViRobot ejecuta distintos tipos de motores para cada familia de virus. Por ejemplo, el motor ViRobot para virus de DOS y Windows, MacRobot para virus de macro, JavaRobot para virus Java y ActiveX y SpyRobot para Troyanos, Backdoors y Spywares; con ésta metodología y el motor de Softwin garantizamos un eficiente rastreo y reparación de virus, aun en archivos comprimidos en diferentes capas y formatos de compresión.



Certificaciones



ViRobot Intranet Security Management System



VISMS es un sistema poderoso y confiable para el Control de Seguridad que aplica de manera integral una profunda administración y protección para la gestión de redes, usuarios y servidores de archivos desde una misma consola, sin importar los diferentes sistemas operativos utilizados. Además, está diseñado para que un solo administrador de red tenga la capacidad de controlar diversos aspectos de seguridad relacionados con Virus, Spyware, Actualizaciones de Seguridad y Procesos Maliciosos, entre otros.

Funciones

• **Políticas para ajustes del nivel de la Seguridad en la Red:** Puede aplicar configuraciones de seguridad a todos los equipos de manera muy sencilla. Un ejemplo de ello es bloquear las infecciones de Virus por medios extraíbles como USB con una configuración simple.

• **Información de las Cuentas de Usuario de Windows:** Indica en tiempo real todos los usuarios que tienen cuenta de usuario Windows con password débil, indicando el mismo, el cual se puede cambiar desde la consola central, evitando con ello pérdida de información y daños al sistema operativo.

• **Información de Hardware y Software:** Realiza Inventarios de Hardware y Software en los equipos con el objetivo de analizar cambios y monitorear posibles vulnerabilidades por programas peligrosos como P2P, también permite ejecutar la desinstalación remota de los mismos.

Integración con Windows Server Update Services

VISMS se integra con WSUS de Microsoft para proporcionar una poderosa herramienta de Administración de Actualizaciones de Seguridad para sus sistemas operativos y aplicaciones de Microsoft, con la ventaja que no requiere de Active Directory (AD), inclusive, si cuenta con él; mejora las capacidades de WSUS al poder incluir la actualización de su equipo.



Herramientas

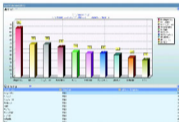
- **Respuesta Emergente para Procesos Maliciosos:** Podemos eliminar algún proceso malicioso en los equipos incluyendo la llave del registro que lo inicia, creando un log de dicha actividad una vez que ésta ha sido resuelta.
- **Envío de Mensajes:** Permite enviar mensajes de índole informativo a los clientes sobre un canal seguro de comunicación.
- **Envío de Archivos:** Permite enviar cualquier tipo de archivo a los equipos de usuarios.
- **Ejecución Remota de Programas:** Permite iniciar de manera remota cualquier ejecutable en sus equipos.
- **Edición Remota de Registro:** Toma control remoto del registro de Windows del equipo cliente desde la Consola de Administración.
- **Administrador de Tareas Remoto:** Ejecuta el Administrador de Tareas con los procesos de otro equipo remotamente.
- **Control Remoto:** Permite tomar control remoto del equipo e iniciar una sesión de chat para dar soporte.
- **Explorador Remoto:** Permite explorar las unidades lógicas de un equipo remotamente.
- **Apagado de Equipos:** Permite apagar, reiniciar o suspender equipos remotamente.

Reportes

Mediante el Reporteador de VISMS se obtiene información de:

- Top 10 e información detallada de virus, spyware, spam, correo electrónico, entre otros.
- Vulnerabilidad por recurso compartido, reglas de bloqueo.
- Inventarios de Hardware y Software.
- Estado actual de instalación, historial de la instalación de la solución Anti-Virus en cada equipo.
- Estadísticas de Incidencias diarias, mensuales.
- Reportes definidos por el usuario.
(creados de acuerdo a las necesidades del cliente)

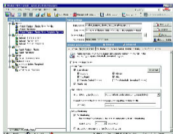
Nota: estas consultas pueden realizarse por departamento, fechas, etc. Todos estos reportes se obtienen de una base de datos MSDE de Microsoft, esto permite generar reportes ejecutivos de alto nivel en los formatos html, excel, txt, xml.



Políticas

Permite definir previamente las reglas de configuración de escaneos, actualizaciones, bloqueos de red, bloqueos de procesos etc.; todo esto desde la consola de administración, éstas son enviadas a los clientes en forma de actualizaciones.

Nota: Pueden ser aplicadas de forma general, por departamento o por usuario, lo cual nos brinda una administración ordenada.



Características

- Fácil y rápida instalación.
- Análisis Remotos cubriendo diferentes puntos de seguridad.
- Información sobre vulnerabilidades de red, explotables por worms.
- Información sobre Carpetas Compartidas en la red.
- Información sobre Actualizaciones Críticas Microsoft Windows.
- Envío de mensajes y archivos a través de la Consola de Administración.
- Ejecuta comandos de forma remota desde la consola.
- Control remoto del registro de Windows.
- Control remoto del escritorio del cliente.
- Explorador remoto de carpetas.
- Apagar, reiniciar o suspender equipos remotamente.
- Perfiles de Usuarios para Administración de Consola (definidos por privilegios).
- Ejecución de tareas programadas.
- Reportes Ejecutivos.

Quién más necesita ViRobot Intranet Security Management System ?

PyMES

Esta solución también es de gran utilidad para las pequeñas y medianas empresas, debido a las características que conforman a VISMS es posible facilitar, centralizar y hacer más eficiente la administración del entorno, todo esto al alcance de cualquier PyME. La relación costo – beneficio tiene un rápido retorno de inversión al trabajar en un ambiente confiable y seguro, logrando una alta disponibilidad de operación y seguridad de la información.

Requerimientos

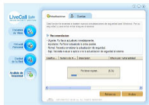
Para Servidor VISMS

Sistema Operativo: Windows 2000 Server / Windows 2000 Advanced Server / Windows 2003 Server.
Procesador: Pentium 1.5 GHz (o superior recomendado).
Memoria: 512 MB (o superior recomendado).
Disco Duro: 1 GB. (o superior recomendado).
Otros: Internet Explorer 6, red para TCP/IP.
Nota: Si se supera los 500 usuarios, se recomienda un Servidor dedicado.

Para Cliente VISMS

Sistema Operativo: Windows Vista / Windows XP / Windows 2000 Professional / Windows NT Workstation (SP 4 o superior recomendado) / Windows ME / Windows 98.
Procesador: Intel Pentium III 500 MHz (o superior recomendado).
Memoria: 128 MB (o superior recomendado).
Disco Duro: 300 MB. (o superior recomendado).
Otros: Internet Explorer 6, red para TCP/IP.

LiveCall Suite



Es una solución de seguridad total en línea, desarrollada para proveer una interfaz intuitiva, de gran desempeño y velocidad que le permite obtener al usuario un ambiente seguro en su PC cuando navega por Internet. Previene el robo de información confidencial mientras lee/esta en su navegador de Internet. También es capaz de detectar e interceptar virus y herramientas de Hackeo que están siendo ejecutadas en su equipo, eliminándolos de la memoria en tiempo real. Adicionalmente LiveCall Suite contiene un conjunto de poderosas herramientas que realizan análisis de vulnerabilidades de seguridad en Windows para carpetas compartidas, cuentas de usuario, monitoreo de programas, puertos y direcciones IP.

LiveCall Suite, la Solución de Seguridad Total en Línea le permite establecer un ambiente seguro para realizar comercio electrónico por Internet.

Características

• LiveCall Suite

Se puede utilizar en cualquier lugar y en cualquier momento, es un producto de seguridad en línea para usarse cómodamente mientras se está conectado a Internet.

• Variedad de funciones

LiveCall Suite cuenta con Anti-Virus, Firewall, Administración de Red y de Seguridad, además muestra información de vulnerabilidades en su PC.

• Actualización Automática

LiveCall Suite se actualiza al último engine automáticamente al conectarse a una PC con acceso a Internet, esto lo mantiene protegido de cualquier amenaza a la seguridad de su equipo.

• Escaneos en Memoria

LiveCall Suite detecta y repara los archivos en memoria al ejecutarse; de la misma manera el escaneo de disco duro detecta y repara los archivos manteniendo su integridad.

• Auto Ejecución

La Función de Seguridad Total es ejecutada automáticamente al ingresar a la página Web donde está configurada.

• Monitoreo de Memoria y Proceso

Mientras que LiveCall Suite está ejecutándose en su PC, mantiene el monitoreo y escaneo de su equipo para proveerle un ambiente de trabajo seguro.

• Compatible con otros productos Anti-Virus

Contrario a otros productos de seguridad Anti-Virus, es posible ejecutar LiveCall Suite mientras otros Anti-Virus se encuentran en ejecución sin intervenir en el buen desempeño de su equipo.

• Poder y desempeño en línea para detectar y reparar virus

LiveCall Suite contiene un poderoso Anti-Virus en línea. Los virus encontrados dentro de una computadora pueden ser detectados y sus daños reparados con el uso del último motor, sin necesidad de tener una versión instalada al utilizar LiveCall Suite.

Quién más necesita LiveCall Suite



Usuarios, Empresas e Instituciones
que requieren de seguridad durante
la navegación por Internet.

Internet es un medio de comunicación que ha revolucionado la manera de hacer negocios, de la misma manera las amenazas a la seguridad se ven multiplicadas y son cada vez más complejas, es por esta razón que esta solución es para cualquier Empresa, Corporativo, Entidad Governamental o Institución Educativa, entre muchos otros, que esté comprometida con la seguridad de sus usuarios y busque darles tranquilidad al proveerle la Solución Integral más completa. La integración a sus portales es muy sencilla y además les brinda la posibilidad de registrar y reportar el cómo los usuarios utilizan la herramienta para una mejor toma de decisiones. Hoy en día aquellas empresas preocupadas por la seguridad son las que más destacan a nivel mundial por su visión y compromiso con sus usuarios, socios y accionistas.

ViRobot Security Suite



ViRobot Desktop es una aplicación de seguridad integral que contiene Anti-Virus, Seguridad de Red mediante un Firewall, Protección de Carpetas, Protección de Correo Electrónico, Anti-Spyware y otras funciones que son desarrolladas por la avanzada tecnología de HAURI para crear un ambiente más seguro cuando usted navegue en Internet.

En el pasado el usuario de una computadora personal podía resolver los problemas del Sistema Operativo simplemente al instalar una actualización de seguridad o una vacuna Anti-Virus, pero en el presente los usuarios deben estar preparados para proteger sus computadoras de los nuevos tipos de programas y códigos maliciosos tales como: BotNets, RootKits, Spywares y Herramientas de Hackeo que están diseñadas para evitar su detección y eliminación.

ViRobot Desktop es el nuevo producto de seguridad total desarrollado para proteger a los usuarios contra Virus, Gusanos o Códigos Maliciosos, Spam, Spyware, etc.; los cuales se distribuyen rápidamente mediante Internet y el correo electrónico causando graves daños.

Funciones

• Bloqueo de Worms y Spam mediante Filtrado de Correos Electrónicos

ViRobot Desktop realiza un monitoreo en tiempo real de correos electrónicos, los cuales son una de las principales rutas de infección que utilizan los virus, escanea los archivos adjuntos en busca de Worms (gusanos), Spam (correo no solicitado) y Scripts (comandos) maliciosos entre otros.

• Análisis de Vulnerabilidades - Parches de seguridad

Muestra un listado de las actualizaciones críticas para el Sistema Operativo que hagan falta de instalar.

• Análisis de Vulnerabilidades - Administrador de Cuentas

Muestra una lista de todas las cuentas generadas en el equipo indicando la seguridad de las mismas.



Protección para programas de Mensajería Instantánea

Cuenta con protección para programas como MSN Messenger, por lo tanto puede bloquear el acceso de archivos potencialmente peligrosos como Virus, Código y Programas Maliciosos que son enviados por equipos infectados a través de sus contactos de mensajería instantánea.



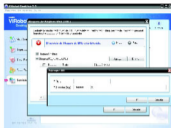
Asistente de Políticas de Seguridad de VIRUSWALL

La función de VirusWall es donde se configuran políticas para protección de Carpetas Compartidas, Procesos, Virus y Red, permite al usuario establecer la seguridad fácilmente y también realizar una configuración detallada. Hace un registro de eventos para facilitar el soporte y verificar su funcionamiento. Mediante estas funciones es posible administrar la seguridad de equipos en red.



System Cleaner

Elimina archivos innecesarios para el sistema, protegiendo su información privada y así evitar el robo de la misma.



Bloqueo de Páginas Web (URL)

Permite Bloquear Sites Web en particular, estos definidos previamente por el Usuario, esto para protección en la Navegación.

Características

• Protege su PC de amenazas mediante un eficaz Bloqueo de Virus

El motor Anti-Virus de ViRobot, desarrollado por la tecnología y experiencia de Hauri, bloquea los programas maliciosos de manera eficiente, brindándole un entorno seguro en su PC.

• Detección y Reparación de Código Malicioso

Para proteger su PC de algún problema de virus, Hauri recolecta y analiza los patrones de Spywares, Adwares, Rootkits, BotNets y otros programas maliciosos, para después actualizar su módulo de detección y reparación, esto le permitirá estar seguro mientras navega en Internet.

• Análisis y Corrección de Vulnerabilidades del Sistema

ViRobot Desktop cuenta con la función de Análisis de Vulnerabilidades donde el usuario puede revisar la información de Actualizaciones de Seguridad para su Sistema Operativo, cuentas de Usuario Locales vulnerables por contraseñas simples y Verificación de Carpetas Compartidas.

• Soporte para Protección de Carpetas mediante Políticas de Seguridad

ViRobot Desktop puede controlar las carpetas compartidas, ejecución de procesos de red y virus con sus avanzadas funciones de control de acceso, el usuario puede activar y configurar fácilmente estas funciones mediante los asistentes de configuración.

• Mejora de la Capacidad de Seguridad al Mínimo Costo

Debido a que ViRobot Desktop contiene funciones de Anti-Virus, Seguridad de Red (para el bloqueo de actividades maliciosas, Hackeo), Protección de e-Mail y funciones de Análisis de Vulnerabilidades en un solo programa de seguridad total, el costo por adquirir protección para los posibles problemas de seguridad se vuelve sumamente atractivo y rentable.

Quién necesita ViRobot Desktop ?

Esta solución Anti-Virus está diseñada para cubrir las necesidades de toda persona que tenga una computadora con conexión a Internet (usuario casero o móvil), con la finalidad de mantener un ambiente seguro y estable en el equipo, lo cual permite mantener la integridad y confiabilidad de su información.

Requerimientos

- **Sistema Operativo:** Windows XP / Windows 2000 Professional / Windows NT Workstation (SP 4 o superior recomendado) / Windows ME / Windows 98 / Windows Vista.
- **Procesador:** Intel Pentium III 500 MHz (o superior recomendado).
- **Memoria:** 128 MB (o superior recomendado).
- **Disco Duro:** 300 MB (o superior recomendado).
- **Otros:** Internet Explorer 6.0 (o superior recomendado), TCP/IP.

ViRobot Windows Server



ViRobot Windows Server es un poderoso Anti-Virus desarrollado para Plataforma de Servidores, el cual integra diferentes Módulos de Seguridad tales como Anti-Virus, Seguridad de Red, Protección de Carpetas, Firewall Personal, Servidor de Actualizaciones, entre otros. Esto hace que Windows Server sea una Solución Completa para Servidores, los cuales requieren de una sólida Seguridad para sus Sistemas. Proteja sus Servidores contra todo tipo de programas maliciosos, ViRobot Windows Server detecta y repara en tiempo real los virus en todo tipo de archivos, incluyendo comprimidos y lo hace antes de que lleguen a los equipos de los usuarios, con lo que permite el intercambio seguro de información, proporcionándole así un ambiente seguro de red.

ViRobot Windows Server también opera como servidor de actualizaciones ya que no solo descarga para sí mismo, también lo hace para los clientes de ViRobot Desktop, con esto es posible centralizar la descarga de actualizaciones desde un solo punto en la red.

Necesidades

Tradicionalmente un producto Anti-Virus común no puede hacerse responsable de toda la seguridad del equipo debido a que un Servidor tiene limitantes para protegerse así mismo y a sus clientes contra nuevos tipos de programas maliciosos. Desde que los virus, gusanos, herramientas de hackeo, etc.; son desarrollados e integran en su rutina maliciosa la tecnología para propagarse rápidamente, nos hace ver que un solo elemento de seguridad no puede controlar este tipo de amenazas a la perfección además de detectarlas y repararlas. Es por eso que las Empresas o Instituciones de Gobierno necesitan de un producto de Seguridad Total para sus servidores como lo es ViRobot Windows Server el cual fue desarrollado para proteger las plataformas de servidores contra virus, gusanos, programas maliciosos, etc.; además cuenta con diversas herramientas de administración.

Características

- Administración Total de Seguridad en las diferentes funciones.
- Análisis de Vulnerabilidades.
- Protección de Carpetas a través de Políticas de Seguridad.
- Actualizaciones del motor del Anti-Virus.
- Soporte a diferentes Sistemas Operativos.
- Seguridad de Red.

Funciones

- Políticas internas de acceso configuradas por el Administrador.
- Centro de soporte para parches de seguridad o recursos compartidos.
- Función de la carpeta cuarentena para archivos infectados.
- Eventos y reportes del servidor, así como errores de operación.
- Estatus de los procesos mediante un escaneo rápido a la carpeta Windows.
- Función de actualizar el Anti-Virus con las últimas definiciones de virus.

Requerimientos

- **Sistema Operativo:** Windows 2003 Server / Windows 2000 Server Windows NT 4.0 Server (SP 6 o superior Recomendado).
- **Procesador:** Pentium III 300 MHz (o superior recomendado).
- **Memoria:** 256 MB (o superior recomendado).
- **Disco Duro:** Espacio mínimo 800 Mb (o Superior recomendado).
- **Otros:** Internet Explorer 5.5 (o superior recomendado), TCP/IP.

ViRobot Mail Security



ViRobot Mail Security bloquea todo tipo de correo malicioso que contenga SPAM y VIRUS de la manera como lo realiza una Solución conjunta de Anti-Spam y Anti-Virus. ViRobot Mail Security tiene un poderoso filtro, que permite crear condiciones para bloquear correo Spam de envío masivo. El administrador puede establecer distintas políticas de seguridad para usuarios utilizando la interfaz de administración vía Web.

Quién necesita ViRobot Mail Security?

Todas aquellas empresas que administren su Servidor de Correo Electrónico. ViRobot Mail Security provee un filtrado robusto contra el Spam basado en una instalación y configuración simple.

Funciones

- **Bloqueo de Correo Malicioso en Tiempo Real**
Con el filtro Spam Inteligente bloquea en tiempo real correo malicioso y con contenido Spam.
- **Políticas basadas en Filtro SPAM**
El Administrador podrá bloquear correo malicioso con solo modificar las configuraciones de las políticas como es dirección IP, remitente, título, texto, nombre de archivo, extensión entre otras.
- **Soporta diversas Plataformas**
Compatible con todos los tipos de Servidores de Correo instalados en plataformas tales como: Windows, Solaris, Linux, FreeBSD entre otras.
- **Integración con la Consola de Administración Hauri**
Integración con VISMS 3.5, si elige VISMS 3.5 y ViRobot Mail Security reduce los costos al manejar una solución total de seguridad incluida la protección para correo.
- **Diferentes formatos de Reportes**
Proporciona diferentes gráficos que se pueden exportar a Excel.
- **Facilidad para Configuración y Operación**
Habilitar la configuración inicial es muy sencillo durante el proceso de instalación así como establecer los servicios con solo seleccionar desde la interfaz gráfica de usuario.

Características

- Filtro SPAM Inteligente.
- Alto índice de detección de SPAM: cerca del 97%.
- Servicio de Filtrado de Correo Electrónico.
- Cuenta con listas blancas/negras.
- SPF (Sender Policy Framework).
- Índice de falsos positivos de SPAM: 1/1,500,000.
- Usa un engine Anti-Spam de CommTouch empresa líder en soluciones Anti-Spam.
- Protección en tiempo real ante nuevos brotes de Spam.

Requerimientos

- **Sistema Operativo:** Linux (x86), Solaris (Sparc), Solaris (x86), FreeBSD (x86).
- **Procesador:** Pentium4 2.8 GHz o superior.
- **Memoria:** 512MB o superior.
- **Disco Duro:** 1Gb o superior.
- **Otros:** Internet Explorer 5.5, Mozilla Firefox 2.x o superior, IPv4/IPv6, 32 bit.

Por qué HAURI?

Soporte Remoto



Beneficios

- Mejoramos considerablemente el tiempo de respuesta técnica.
- No tenemos límites de distancia ya que el soporte es vía Web.
- Permite al usuario final tener contacto directo con especialistas en las tecnologías de Hauri.
- Nos permite una retroalimentación técnica directa con el usuario final.
- No es necesario abrir puertos de comunicación en la configuración de su Firewall Perimetral.
- Puede ser utilizado vía Web en conexiones a Internet desde 64kbps.

Contamos con diferentes Líneas de Soporte Técnico

• LiveChat

Conoce nuestra nueva herramienta de soporte y resuelve tus dudas técnicas en tiempo real a través de nuestra página: www.hauri-la.com

• NextSupport

Todas nuestras sucursales cuentan con equipo de Radiocomunicación Nextel para un rápido y efectivo contacto con el equipo técnico.

• Foro Técnico

Visite nuestro Foro Técnico y consulta tus dudas técnicas al momento.
foro.hauri-la.com

Hauri University



- Hauri provee cursos gratuitos sobre sus soluciones de seguridad para redes.
- Los cursos son ofrecidos en salas de capacitación equipadas para proveer una interacción directa con la aplicación generando un aprendizaje inmediato.
- Las salas de capacitación están ubicadas estratégicamente para proveer cobertura a nivel Latinoamericano.
- Para mayor información consulte en www.hauri-la.com zona de Soporte en Cursos y Eventos.



END POINT TOTAL SECURITY SERVICE



www.hauri-la.com

atencion@hauri-la.com

soporte@hauri-la.com