BITDEFENDER CLIENTE SEGURIDAD

BASES DE SEGURIDAD DE UNA COMPAÑÍA

Los requisitos de seguridad para cualquier empresa nueva o ya existente – no importa cuán grande o pequeña sea – deben ser los mismos. Mientras que proteger la propiedad intelectual de su empresa y asegurar los datos del cliente son buenas prácticas empresariales, el impacto de cualquier ataque virus puede afectar en gran medida a la eficacia operativa de la empresa y puede incurrir en una pérdida de la productividad en el trabajo. Esta pérdida de productividad puede paralizar una empresa pequeña y, en el mejor de los casos, obstaculizar el crecimiento de la misma.

MÁS QUE UN SIMPLE ANTIVIRUS

Las amenazas están en constante evolución con el objetivo de eludir los controles de seguridad de su empresa. Mientras que un antivirus es la base de una buena política de seguridad, no debe ser la única respuesta a la protección de su trabajo frente a amenazas maliciosas. Entre las amenazas que causan interrupciones importantes en su negocio puede encontrar:

Virus. Transmitidos vía infección de archivos ejecutables, ocultos dentro de archivos comprimidos o como macros en documentos legítimos. Entre las acciones destructivas de un virus podemos encontrar el borrado de archivos, cifrado de datos, borrado de disco duro, etc.

Adware/Spyware. Casi tan prejudicial y peligroso como un virus, el spyware puede ser difícil de identificar y eliminar. La fuga de datos personales y corporativos debe ser una preocupación clave, al igual que el deterioro del rendimiento del equipo, la instalación de software adicional no deseado y el redireccionamiento forzado de la actividad web. Los sistemas infectados gravemente pueden requerir una reinstalación completa del sistema, perdiendo horas y recursos de TI.

Gusanos. Un programa autorreplicante que utiliza la red para propagarse haciéndola más lenta e infectando los sistemas aprovechando sus vulnerabilidades y las de las aplicaciones. Las acciones que se derivan de su infección pueden incluir desde el borrado o cifrado de archivos y el envió de documentos por e-mail, hasta la instalación de puertas traseras (backdoors), zombies y troyanos.

Troyanos y rootkits. Los troyanos y rootkits parecen ser programas legítimos, pero están diseñados para permitir el acceso remoto a un sistema informático. Una vez que un troyano o un rootkit se instala, un atacante podrá acceder remotamente al sistema y podrá sustraer datos. Detectar y prevenir este tipo de amenazas manualmente puede llevar mucho tiempo y a menudo conducen a una reinstalación completa del sistema si no se eliminan correctamente.

E-mail Spam y Phishing. Los anuncios comerciales no solicitados distribuidos a través del correo electrónico son algo más que una molestia. El spam consume demasiado tiempo personal si no se gestiona apropiadamente. Algunos ataques de spam o phishing también pueden incluir malware adjunto – que lleva a comprometer la seguridad empresarial interna si se ejecuta – o enlaces a sitios web que solicitan información personal. El phishing utiliza técnicas similares pero dirige al usuario a un sitio web aparentemente legítimo para recopilar información personal, como la referente a cuentas bancarias o tarjetas de crédito o instala keyloggers en el sistema que pueden sustraer información sensible de la empresa.

El impacto del malware puede ser un trastorno grave para todos en la empresa – sin embargo, es en el departamento de TI donde se notan más las consecuencias. Los administradores de TI que se ocupan de la eliminación de un gusano de rápida propagación o de un virus que ha infectado un gran número de sistemas, saben que esta es una acción larga que conlleva mucho tiempo. Desgraciadamente, esta tarea debe tener preferencia frente a otros proyectos de TI para evitar la pérdida de datos y restaurar la eficiencia del trabajo lo más rápidamente posible.

CARACTERÍSTICAS PRINCIPALES Y BENEFICIOS

- Galardonada detección, limpieza y cuarentena de virus.
- Permite la programación flexible de ejecuciones de análisis inmediato o bajo demanda para evaluar las infecciones al día.
- Análisis optimizado mediante el uso de archivos de huella para cada sesión de usuario, que reanaliza en cada nueva sesión, en actualizaciones o en una infección del sistema.
- Cuarentena de archivos infectados o sospechosos para minimizar infecciones y garantizar posteriores análisis seguros.
- Administración y configuración basadas en políticas.
- Protección cortafuego personal para usuarios remotos y móviles.
- Análisis de dispositivos extraíbles y políticas de control de acceso.
- Protección antispam a nivel de sistema con actualizaciones constantes, lista blanca / lista negra y motor de aprendizaje Bayesiano para identificar nuevos tipos de spam que traspasan los filtros tradicionales.
- Filtro de contenido personalizable para identificar información sensible a la hora de minimizar los riesgos de fuga de información.
- Hacer cumplir la seguridad con perfiles de acceso a la interfaz limitados y desinstalaciones protegidas con contraseña.
- Reducción de los costes de recursos y gastos generales para la gestión de múltiples clientes utilizando una consola de administración centralizada.
- Permite la configuración remota, auditoría, instalación y desinstalación de aplicaciones de cualquier sistema cliente o servidor en la red.

bitdefender

TECNOLOGÍAS BITDEFENDER

AVC BitDefender Active Virus Control es una tecnología de detección proactiva innovadora que utiliza avanzados métodos heurísticos para detectar nuevas amenazas potenciales en tiempo real. Monitoriza cada programa en ejecución en su equipo, a la vez que ejecuta y descubre acciones propias del malware. Si se detectan suficientes de estas acciones, el programa que las lleva a cabo se declara dañino.

b-have Todas las soluciones BitDefender incluyen B-HAVE, tecnología pendiente de patente, que analiza el comportamiento de códigos potencialmente peligrosos dentro de una máquina virtual, eliminando así los falsos positivos y aumentando significativamente la tasa de detección frente a malware nuevo y desconocido.

NeuNet Para combatir mejor las nuevas oleadas de spam, los laboratorios de BitDefender han creado el potente filtro antispam NeuNet. En los laboratorios antispam, NeuNet es preentrenado sobre una serie de mensajes para que aprenda a reconocer el nuevo tipo de spam percibiendo sus similitudes con los mensajes que ya ha examinado.

REQUISITOS DEL SISTEMA

La solución BitDefender Client Security se presenta con administración centralizada del lado del servidor y componentes de protección de puestos finales del lado del cliente. La parte del cliente incluye dos componentes: BitDefender Business Client para proteger y controlar los puestos finales Windows, y BitDefender Agent para activar la administración centralizada. Los componentes del lado del cliente se implementan utilizando la plataforma de administración centralizada de BitDefender.

BitDefender Business Client y Management Agent

Procesador Intel Pentium compatible:

- 500 MHz para Windows 2000
- 800 MHz para Windows XP
- 1 GB para Windows Vista y Windows 7

Memoria RAM:

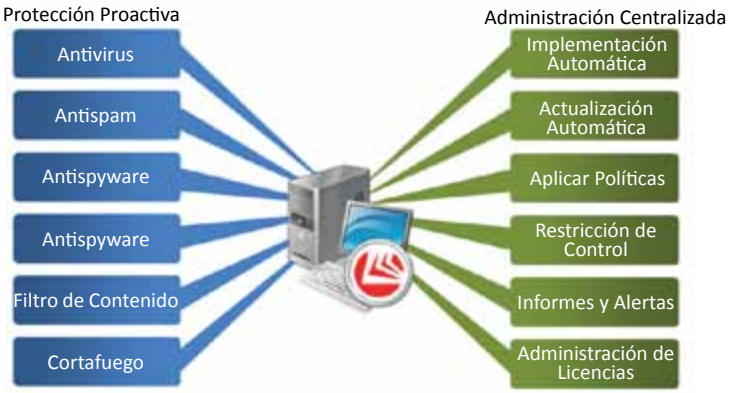
- 512 MB para Windows 2000, Windows XP
- 1 GB para Windows Vista y Windows 7

Espacio en disco mínimo:

- 300 MB (400 MB para la instalación)

Sistema operativo:

- **Business Client y Management Agent** para Windows 7, Windows Vista SP1, Windows XP (SP2), Windows Home Server, Windows 2000 Professional (SP4 Rollup 1 v2)
- **Management Agent** también para Windows 2008 / 2008 SBS / 2008 R2, Windows Server 2003 (SP2), Windows 2000 Server (SP4 Rollup 1 v2), Mac OS X 10.4.6 o posterior, Linux 2.4.x o 2.6.x con glibc 2.3.1 o posterior y libstdc++5 de gcc 3.2.2 o posterior



BitDefender Client Security ofrece múltiples niveles de protección y funcionalidades a la hora de administrar los clientes

PROTECCIÓN PROACTIVA DE ÚLTIMA GENERACIÓN

Los galardonados motores de análisis de BitDefender han sido reconocidos por los principales organismos de certificación – entre ellos, ICSA Labs, Virus Bulletin y West Coast Labs – por su excelente protección proactiva antimalware.

BitDefender Client Security ofrece múltiples niveles de avanzada protección: antivirus, antispam, antispyware, antiphishing, filtrado de contenido, detección de troyanos/rootkit y un cortafuego personal con todas las funciones. Todas las funciones son configurables de forma remota, incluyendo avanzadas políticas de seguridad para controlar el acceso de los usuarios a los dispositivos extraíbles, aplicaciones locales o limitación del tiempo de uso de Internet.

ADMINISTRACIÓN Y CONFIGURACIÓN DEL ANÁLISIS GRANULAR

BitDefender Client Security proporciona múltiples formas de análisis para detectar código malicioso y salvaguardar la integridad de los portátiles y equipos desplegados en la red. Diferentes opciones de análisis ayudan a mantener la integridad del sistema mientras minimizan el impacto de la experiencia del usuario.

On Access. Motor de análisis en tiempo real para la detección de virus en el mismo momento en el que un usuario añade o recupera un documento de una lista o librería de documentos.

La característica de análisis Bajo Demanda permite crear análisis de sistema programado para ejecutarlo fuera de las horas de trabajo sin afectar al rendimiento global o disponibilidad del sistema.

La Configuración del Análisis Programado proporciona programación de eventos configurable para su análisis bajo demanda y tareas de actualización, minimizando cualquier impacto potencial en Servidores o interrupción del Sistema durante las horas de funcionamiento críticas.

Cuarentena de Archivos Infectados o Sospechosos. Los archivos sospechosos se aíslan en zonas de cuarentena. Los archivos pueden ser limpiados o conservados en una zona de cuarentena para su análisis, siendo restaurados a su ubicación original una vez validados, o enviados directamente a los laboratorios antivirus de BitDefender para su evaluación.

INTEGRACIÓN CON LA PLATAFORMA DE ADMINISTRACIÓN CENTRALIZADA DE BITDEFENDER

Un gran número de equipos puede ser administrado de forma rápida y fácil a través de la plataforma de administración centralizada de BitDefender, dando a los administradores de TI visibilidad de las amenazas malware en toda la empresa y la capacidad de proteger proactivamente sus recursos de red. BitDefender Management Console proporciona un punto centralizado para la instalación remota, configuración y presentación de informes de todos los clientes BitDefender, además de todas las soluciones para servidor y puertas de enlace desplegados en la red.

vb 100 VIRUS virusbtn.com

Compatible with Windows 7

bitdefender