



Solución integral para endpoints corporativas con varias capas de protección de antivirus, antispyware, firewall y control Web. La administración remota facilita y acelera la supervisión de la seguridad, desde una única consola.

Requerimientos del sistema:
Windows® 8 y 7, Vista, XP, 2000, NT 4.0 (SP6), Windows Server 2000, 2003, 2008, 2008 R2

Arquitectura del procesador:
Intel®/AMD® x86/x64

Antivirus y antispyware	Elimina todos los tipos de amenazas, incluyendo virus, rootkits, gusanos y spyware, y mantiene la red protegida esté o no en línea. La exploración opcional basada en la nube utiliza nuestra base de datos de reputación de archivos para lograr la máxima velocidad de exploración y la mínima tasa de falsos positivos.
NUEVO Sistema de prevención de intrusiones basado en el host (HIPS)	Proporciona protección ante la manipulación indebida y protege el registro del sistema, los procesos, las aplicaciones y los archivos ante modificaciones no autorizadas. Es posible personalizar el comportamiento del sistema hasta en el más ínfimo detalle e incluso detectar las amenazas desconocidas por su conducta sospechosa.
NUEVO Control Web	Permite limitar el acceso mediante la selección de categorías de sitios Web basada en la clasificación automática en la nube. Regule y controle las páginas Web a las que acceden los usuarios o grupos de usuarios, mediante diversas categorías de sitios Web (juegos, redes sociales, sitios web maliciosas, compras, entre otros).
Detección de red de confianza	Permite definir redes de confianza y proteger todas las demás conexiones con el modo estricto para que los equipos portátiles permanezcan invisibles en redes Wi-Fi públicas en hoteles, aeropuertos y conferencias.
Firewall bidireccional	Previene el acceso no autorizado a la red de la empresa y protege los datos corporativos ante su exposición. La administración remota proporciona un asistente de fusión de reglas del firewall que simplifica el agregado de reglas de firewall en la red.
Antispam del cliente	Protege las comunicaciones de la empresa ante spam y amenazas provenientes del correo electrónico. Configure listas blancas y negras así como el autoaprendizaje para cada cliente o grupo en forma separada. El antispam soporta Microsoft Outlook en forma nativa y también filtra los protocolos POP3, IMAP, MAPI y HTTP.
NUEVO Control de dispositivos	Permite bloquear medios y dispositivos no autorizados según reglas y parámetros predefinidos, tales como CD-ROM, FDD, Bluetooth, cámaras, modems, LPT/COM, impresoras, teléfonos, etc. Se puede configurar por permisos de acceso (lectura/escritura, lectura, bloqueo) para medios, dispositivos, usuarios y grupos individuales. También es posible especificar accesos por marca, modelo, serie. Todo esto se puede realizar desde la consola de administración, además de poder identificar cuando se conecta algún dispositivo sin autorización.
NUEVO Instalación basada en componentes	Instale alguno de los siguientes componentes de seguridad, o todos ellos: firewall, antispam, control Web, control de dispositivos, Soporte para NAP de Microsoft y protección del acceso a la Web. También es posible habilitar o deshabilitar los módulos instalados en forma remota.
Bajo impacto en el sistema	Asegura la protección comprobada a la vez que deja disponibles más recursos del sistema para los programas que usa a diario. Nuestro software también se ejecuta en forma fluida y sin problemas en hardware más antiguo, lo que le ahorra el tiempo y el gasto de tener que actualizar las endpoints.
NUEVO Varios formatos de registros	Guarde registros en formatos comunes (CSV, texto sin formato o registros de sucesos de Windows) para su análisis o recopilación inmediatos. Aproveche las ventajas de que las herramientas SIEM de terceros puedan leer los datos; RSA enVision cuenta con soporte directo mediante un complemento.