LICITACIÓN PÚBLICA N° 15/2023 PJ – SIAFyC
"Adquisición de Software de Antivirus para el Poder Judicial"

Especificaciones Técnicas

Anexo

Software de Antivirus

Características generales mínimas

Software de antivirus corporativo para estaciones de trabajo y servidores.

Características tecnológicas

- La solución deberá poder realizar exploraciones en estado inactivo para poder brindar de esa forma, una protección proactiva mientras el equipo no está en uso.
- Debe tener un caché local para aumentar el rendimiento de los entornos virtuales, garantizando que el archivo sólo se explora una vez.
- El producto debe tener un control web para limitar el acceso a los sitios web por categoría, además de poderle mostrar al usuario una notificación de bloqueo.
- El bloqueo web deberá poder asignarse por un rango de tiempo, por grupo y por equipo.
- Deberá tener la capacidad para verificar el estado de actualizaciones de seguridad del sistema operativo.
- Dentro del módulo de firewall deberá contar con la funcionalidad de bloqueo de exploits.
- La solución debe ser capaz de permitir o negar el uso de los dispositivos externos en base a los siguientes criterios:
    - Fabricante
    - Modelo
    - Número de serie
- La solución debe ser capaz de definir un listado específico de usuarios quienes pueden hacer uso de los dispositivos. Para dispositivos de almacenamiento, la solución debe permitir configurar como mínimo de los siguientes permisos:
    - Lectura/Escritura
    - Bloqueo
    - Solo de lectura
    - Advertir
- Cuando se conecta o usa un dispositivo de almacenamiento, la solución de antivirus debe proporcionar las siguientes opciones:
    - Escanear
    - No realizar ninguna acción
    - Recordar esta acción
- Sistema de prevención de intrusiones basado en el host (HIPS)
- La solución debe tener sistema de prevención de intrusiones basado en el host. El sistema HIPS debe tener los siguientes modos de configuración:

    - Modo automático
    - Modo inteligente
    - Modo interactivo
    - Modo basado en políticas
    - Modo aprendizaje
- Debe permiter aislar un equipo de la red de datos.
- La solución debe capaz de verificar las conexiones bajo protocolo SSL para hallar amenazas.
- Firewall personal, la solución de antivirus debe contar con un firewall personal. El firewall debe tener los siguientes modos de configuración:
    - Modo automático
    - Modo interactivo
    - Modo basado en políticas
    - Modo aprendizaje
- Las reglas de firewall creadas deberán ser capaces de permitir todas las siguientes acciones:
    - Denegar
    - Permitir
    - Preguntar

Consola

- Deberá permitir la ejecución remota de scripts, batch files y paquetes personalizados a través de la consola, de terceros.
- Deberá ser una solución que pueda ser usada y sea administrable desde la consola de antivirus en sistemas operativos Windows.
- Debe permitir generar grupos de clientes dinámicos y grupos estáticos.
- Debe contar con desinstalador de antivirus de terceros.
- Debe contar con características que permitan detección y protección contra ransomware.
- La solución debe permitir realizar instalaciones de consolas distribuidas de administración de clientes. Debe permitir consolidar las auditoría y control en un tablero de comandos centralizado.
- La solución debe tener el mecanismo para desinstalar otras soluciones antivirus presentes en el equipo final.

Seguridad de Archivos

- La solución de protección en servidores debe incluir la detección y bloqueo de intrusiones, agregar a lista negra aquellas direcciones que han sido identificadas con este comportamiento malicioso.
- La solución deberá permitir definir exclusiones que correspondan a aplicaciones necesarias en los servidores y equipos de usuario final.

Análisis en línea de archivos

- Deberá incluir herramientas para análisis de archivos.
- Es posible crear una exclusión por ruta, detección y su hash
- Deberá contar con capacidad de detección de correo SPAM.
- Debe tener protección proactiva, es decir, que el archivo/ejecutable sea bloqueado hasta recibir el resultado del análisis.

Cifrado de datos en equipos

- La solución deberá ser capaz de cifrar los equipos.
- La solución deberá contar con opciones de recuperación de claves de acceso para usuarios remotos.
- La solución deberá poder programar las tareas de cifrado sobre los equipos.
- La solución deberá poder ser administrada desde la misma consola central.

Condiciones para el Fabricante

- Contar con al menos 10 años en servicios específicos de seguridad informática.
- Deberá contar con soporte en Argentina en forma directa del fabricante o partner certificado disponible 7x24.
- Disponer de un laboratorio de análisis y detección de malware.

Implementación y Capacitación

El oferente deberá brindar asistencia para llevar a cabo la implementación de la solución. Deberá ofrecer soporte para instalar el 10 % de los equipos, transmitiendo este conocimiento a personal de la Secretaría de Informática Jurídica.

Cantidad de licencias

- Judicatura: 1560
- Ministerio Público Fiscal: 624
- Ministerio de la Defensa Pública: 420

Vigencia del licenciamiento

Tres años a partir de la entrega del producto.

Performance e Infraestructura

A solicitud de la SIJ se deberá contar con la posibilidad de evaluar el software en referencia a la performance e integraciones a la infraestructura de datos del Poder Judicial. Una vez evaluado el producto se elevará un informe técnico aprobando o desaprobando la solución propuesta.

Software de referencia

TDR ESET Protect Advanced (ESET Dynamic Endpoint Protection)