ESPECIFICACIONES TÉCNICAS PARA EL LICENCIAMIENTO DE ANTIVIRUS PARA LA UNIVERSIDAD DE CUNDINAMARCA
Defensa básica
Protección contra virus, programas troyanos y gusanos.
Protección contra programas espía y publicitarios.
Análisis de ficheros en modo automático o según horario, debe facilitar recursos para otras aplicaciones durante el análisis.
Análisis del correo electrónico mínimo para protocolos: POP3, IMAP, NNTP y SMTP.
Análisis y control de archivos adjuntos por extensión en correo electrónico.
Permitir configurar un salto en el análisis de archivos grandes en correo electrónico según el tamaño que pueda definir el administrador.
Permitir configurar un salto en el análisis de archivos en correo electrónico cuyo análisis tome más de un tiempo determinado según defina el administrador.
Permitir configurar un salto en el análisis de archivos adjuntos en correo electrónico.
Análisis de virus de Internet (para cualquier navegador de Internet).
Permitir la configuración de acciones automáticas ante eventos de posible infección de malware por Internet.
Análisis de tráfico de Internet mínimo para los protocolos: HTTP y FTP.
Análisis y desinfección automática el contenido de los dispositivos de memoria
Que permita acceder a la base de datos del fabricante para revisar reputación de archivos, recursos web, y software
Permitir la creción de URL´s de confianza.
Protección contra acceso de Phishing.
Análisis y defensa para mensajeros instantáneos.
Permitir análisis heurístico de mensajes enviados y recibidos por los servicios de mensajería instantanea.
Rapidez de Escaneo mediante el uso de tecnologías iChecker e iSwift.
Actualizaciones automática de firmas mínimo cada 4 horas.
Chequeo y desinfección de malware contenido en archivos comprimidos.
Cuarentena para archivos infectados.
Chequeo y desinfección de malware contenido en memoria.
Chequeo y desinfección de malware contenido en el sector de arranque.
Detección y desinfección en tiempo real de virus residentes.
Reconocimiento de virus por su forma de empaquetamiento.
Defensa proactiva contra los nuevos programas maliciosos (Día Cero).
Firewall personal.
Firewall debe permitir crear reglas para filtrado de aplicaciones.
Firewall debe permitir crear reglas para filtrado de paquetes.
Firewall debe permitir configurar las diferentes redes como: local, público o de confianza.
Debe tener un módulo de protección contra ataques de red.
Debe permitir crear excepciones en el módulo de protección contra ataques de red.
Administración
Administración y Monitoreo Centralizados.
Dashboard con información de estado del producto en los clientes.
Integración con directorio activo.
Manejo de consolas esclavas por jerarquía con mínimo 10 niveles de anidación.
Licenciamiento ilimitado de consolas y servidores de administración.
Manejo de grupos jerárquicos de usuarios.
Administración Basada en roles.
Capacidad de Administrar servidores y clientes Linux y clientes Mac a través de la consola de administración.
Administración centralizada del antivirus mediante políticas.
Calendarización de tareas tanto de análisis como de actualización.
Permitir detener o activar escaneo de virus PCs individuales, desde la consola.
Capacidad de recibir notificaciones sobre nuevas versiones de las aplicaciones corporativas del producto.
Permitir sincronización de la estructura de Active Directory con la de los grupos de administración.
Permitir la asignación automática de los agentes de actualización.
Permitir soporte de modo dinámico de Virtual Desktop Infrastructure (VDI).
Permitir establecer intervalos de tiempo para la transferencia de datos desde el Agente de Red al Servidor.
Bloqueo del endpoint con contraseña para evitar cambios no autorizados.
Permite envío automático de reportes a usuarios específicos de correo.
Reportes exportables mínimo a HTML, PDF y XLS.
Debe permitir la personalización de nuevos reportes.
Multicasting.
Debe poder cambiar automáticamente la configuración de los endpoints al detectar un brote de virus en la red.
Análisis de conexiones cifradas.
Backup automático y calendarizado de configuraciones completas.
Notificaciones de grupos de estaciones a usuarios específicos de correo.
Capacidad para administrar más de 5.000 dispositivos sobre un mismo hardware
Capacidad de visualizar de manera consolidada los dispositivos gestionados, sus características técnicas, como sistema operativo y versión, Nombre de dispositivo y dirección IP, Tipo de procesador, Tipo de infección
La consola de administración debe permitir manejar múltiples políticas de seguridad, pudiendo activar una política específica ante epidemias de virus
Permitir crear políticas especiales para usuarios móviles
Controlar a través de políticas todos los componentes mencionados previamente (para estaciones de trabajo y servidores), sin necesidad de consolas adicionales de administración
Delegación de tareas mediante la creación de usuarios con distintos perfiles de administración
Permitir la realización de backups de las configuraciones realizadas en el sistema.
Comunicación Cifrada o SSL entre servidores y clientes, a través de certificados digitales propios o de terceros
La consola debe permitir la creación de usuarios y perfiles específicos para ejecutar tareas de control o auditoría específicas por parte del personal de Infraestructura y Riesgo Tecnológico, sin que esto afecte las tareas realizadas por el Administrador de la consola.
Distribución de agentes, configuraciones y actualizaciones de forma centralizada
Facilidad para accesar a la consola desde cualquier sitio en la red
Monitoreo permanente y generación reportes de eventos en tiempo real
Permite desde sitio central la distribución masiva del agente
Facilidad en la actualización del agente para usuarios fuera de la red
Establecer políticas por grupos de trabajo y estructuras de herencia
Desactivar y desinstalar el agente de manera segura y remota.
Consola MMC y Web
Base de datos SQL o My SQL
Compatibilidad con Sistemas Operativos Windows 32 y 64 bits
Windows 10
Windows 8.1
Windows 2003
Windows 2008
Windows 2012
Windows 2016

Compatibilidad con Sistemas Operativos Linux 32 y 64 bits
Sistemas Operativos de 32-bit:
Ubuntu 14.04.5 LTS
Ubuntu 16.04.4 LTS
Ubuntu 17.10.1
Red Hat® Enterprise Linux® 6.9
CentOS-6.9
Debian GNU/Linux 8.10
Debian GNU/Linux 9.4
AltLinux 8.0.0
AltLinux 8.2*
GosLinux 6.6**
Linux Mint 18.3 and later
Lotos (kernel 4.14)
Sistemas Operativos de 64-bit:
Ubuntu 14.04.5 LTS
Ubuntu 16.04.4 LTS
Ubuntu 17.10.1
Ubuntu 18.04
Red Hat® Enterprise Linux® 6.9
Red Hat® Enterprise Linux® 7.4
Red Hat® Enterprise Linux® 7.5
CentOS-6.9
CentOS-7.4
CentOS-7.5
CentOS-7.6
Debian GNU/Linux 8.10
Debian GNU/Linux 9.4
OracleLinux 7.4
SUSE® Linux Enterprise Server 12 SP3
openSUSE® 42.3
AltLinux 8.0.0
AltLinux 8.2*
GosLinux 6.6**
EMIAS 1.0
Amazon Linux AMI 2017.09 or later
Linux Mint 18.3 and later
Astra Linux Special Edition 1.4
Astra Linux Special Edition 1.5
Lotos (kernel 4.14)
Compatibilidad con Sistemas Operativos Mac
macOS Mojave 10.14
macOS High Sierra 10.13
macOS Sierra 10.12
Mac OS X 10.11 (El Capitan)
Mac OS X 10.10 (Yosemite)
Mac OS X 10.9 (Mavericks)
Otras Características
Debe permitir realizar una Instalación 100% Remota
Debe proteger los archivos de instalación a fin de evitar que se corrompan durante la instalación en un equipo infectado
En servidores de multiprocesador, definir el número de copias del motor del antivirus que se quiera ejecutar simultáneamente para acelerar el proceso de los requerimientos del servidor.
Detección mínima de falsos positivos o falsos virus.
Optimizado para usuarios móviles.
La herramienta de seguridad debe tener certificación ISO 9001, que valide la asistencia técnica a nivel de Latinoamerica.
Funciones adicionales
Inventario básico de software.
Debe poder desactivar el arranque automático de dispositivos extraíbles.
Monitoreo de paquetes enviados por la red.
Soportar arquitectura de Clusters.
Registrar los eventos asociados con la eliminación y el guardado de archivos en dispositivos USB.
Generar una lista de redes Wi-Fi confiables según la siguiente configuración: nombre, tipo de cifrado y tipo de autenticación
Controlar las descargas de los módulos y controladores DLL
Que sea optimizado para servidores de multiprocesadores basados en la tecnología Intel Xeon.
Endpoint
Permitir a usuarios seleccionados y / o grupos de usuarios iniciar aplicaciones.
Bloqueo de usuarios seleccionados y / o grupos de usuarios para el uso de las aplicaciones de inicio.
Control de privilegios de aplicaciones que controle la actividad de las mismas para el uso de recursos informáticos
Control por tipo de dispositivo a ser conectado
Permitir a los usuarios seleccionados y / o grupos de usuarios acceder a determinados tipos de dispositivos durante períodos específicos de tiempo.
Permitir a los usuarios seleccionados y / o grupos de usuarios ver el árbol de carpetas en dispositivos de memoria.
Permitir a los usuarios seleccionados y / o grupos de usuarios leer el contenido de los dispositivos de memoria.
Permitir a los usuarios seleccionados y / o grupos de usuarios modificar el contenido de los dispositivos de memoria.
Permitir la creación de dispositivos de confianza a los cuales los usuarios tienen acceso total en todo momento.
Control de acceso web para usuarios y / o grupos de usuarios.
Control de acceso web mediante filtro por categoria.
Control de acceso web mediante filtro por tipos de archivos.
Control de acceso web mediante filtro por categoria y tipos de archivos.
Control de acceso web mediante filtro por direcciones URL.
Control de acceso web mediante reglas para determinados nombres de usuarios y / o grupos de usuarios.
Permitir configurar las reglas de control de acceso web mediante horario.
Permitir dar prioridad a cualquiera de las reglas de control de acceso web creadas.
Permitir configurar las reglas de control de acceso web para: permitir, bloquear o alertar el acceso a los diferentes sitios.
Control de acceso web debe tener un diagnóstico de reglas.
Que permita acceder a la base de datos del fabricante para revisar reputación de archivos, recursos web, y software
Funcionalidades de Cifrado
Cifrado de dispositivos extraíbles o removibles
Cifrado de disco duro (full disk encryption: master boot record, OS, system files)
Cifrado a traves de Bitlocker de MS
Cifrado a traves de Filevault de OSX
Cifrado de archivos y carpetas
Cifrado de dispositivos extraíbles (USB)
Administración centralizada de políticas y llaves
Protección de acceso (Autenticación y Autorización) – Preboot-Authentication
Opciones de recovery de datos (posibilidad dde recuperar contrasenias extraviadas, creacion de usuarios generales)
Cifrado de Tipos de archivos para aplicaciones (y decifrado)
El cifrado debe permitir realizar SSO (inicio de sesion unico con credenciales de Active Directory)

Vulnerabilidades
Generación de informes de amenazas de vulnerabilidad en las aplicaciones, con puntuaciones o niveles de severidad que ayudan a adoptar decisiones para protección de las estaciones.
Desplegar a través de la solución, los parches o actualizaciones que remedien las vulnerabilidades detectadas.
Posiblidad de definir parcheo autmatico para grupos de aplicaciones tanto de Microsoft como de software comercial
Posibilidad de definir grupos de prueba para verificar efectividad de parches.
Mostrar las actualizaciones por instalar e instaladas asi como tambien las vulnerabilidades detectadas en los equipos.
Control de aplicaciones
Brindar la posibilidad de monitorear y controlar las aplicaciones, permitir y denegar el acceso a determinadas llaves del registro, archivos y carpetas.
Poder definir cuales aplicaciones están permitidas para ejecutarse, cuales aplicaciones pueden hacer llamados a Dynamic Link Libraries(DLL).
Brindar visibilidad de las aplicaciones que el usuario ha instalado en los equipos
Flexibilidad para aplicar políticas de control por grupos de usuarios, para permitir o bloquear aplicaciones en particular.
Poder manejar el inventario de aplicaciones agrupado ya sea por todos los archivos binarios (.exe,.dll, controladores y secuencias de comandos), por aplicación y fabricante.
Brindar la posibilidad de clasificar por categorías las aplicaciones por ejemplo: fiables conocidas, desconocidas y maliciosas conocidas.
Poder crear listas blancas y listas negras para especificar qué aplicaciones se pueden ejecutar y cuáles no.
Funcionalidades de Administración de Sistemas
Capacidad de realizar instalación remota y flexible de software con despliegues programados o manuales
Envio de mensajes a usuarios
Apagado, reinicio y encendido de los equipos mediante Wake on LAN a traves de servidor de administracion
Capacidad de creación, almacenaje, clonado y despliegue de imágenes del sistema desde un lugar central
Capacidad de realizar instalación remota y flexible de software de terceros con despliegues programados o manuales
Poder brindar soporte remoto desde la consola en modalidad de escritorio compartido
Soporte para servicios de actualizacion de Servidores Microsoft Windows (WSUS)
Capacidad de sincronizar datos de manera regular con actualizaciones disponibles y hotfixes de servidores, para posteriormente distribuirlos
Capacidad de poder llevar un control de licenciamiento global de aplicaciones

ING. EDILSON MARTINEZ CLAVIJO
DIRECTOR DE SISTEMAS Y TECNOLOGÍA
DIRECCIÓN DE SISTEMAS Y TECNOLOGÍA

ING. PAOLA ANDREA RAMIREZ
PROFESIONAL DIRECTOR DE ÁREA I
DIRECCIÓN DE SISTEMAS Y TECNOLOGÍA