Trabajo Final de Grado

Configuración y Administración de un Sistema Antivirus Centralizado.

Febrero-Junio 2018

Estudios de Informática, Multimedia y Telecomunicaciones.

Alumno: Francisco Javier García Moreno.

Tutor: D. Manuel Jesús Mendoza Flores

Dedicado a mis hijas,

por reclamarme siempre su cuento antes de dormir y así

ayudarme a no perder la capacidad de imaginar,

y a mi mujer por su cariño y comprensión

durante las horas dedicadas a este proyecto.

Sumario

Índice de ilustraciones

Índice de tablas

1. Sumario

La definición del entorno de desarrollo de un proyecto de tecnologías de la información y comunicación (TIC) afecta notablemente a las cuestiones técnicas del mismo, no es posible utilizar reglas lineales, a medida que el escenario de aplicación crece, llega un momento en el cual las metodologías y soluciones deben transformarse para poder ser gestionadas y manejadas correctamente a partir de un volumen alto.

Los entornos Enterprises (empresariales) o Gubernamentales, se caracterizan no solo no por un volumen alto de recursos, también por aspectos como la distribución geográfica, departamental, etc, que implica una serie de retos a cumplir desde el punto de vista tecnológico, como son por ejemplo que cualquier despliegue o mantenimiento que deba llevarse in-situ supondrá un gran coste, por lo que deberán de ser evitados.

Este documento se centra en desarrollar y justificar una solución de antivirus centralizada en dichos entornos, y las ventajas que una arquitectura de este tipo proporcionan a estas corporaciones, teniendo en cuenta los grandes riesgos en seguridad informática a la que se ven expuestas en esta sociedad de la comunicación global donde no cabe cerrar las puertas como medio de defensa.

2. Alcance

2.1. Justificación

La seguridad informática es unos de los campos que mayor crecimiento tendrá en los próximos años, hoy en día afecta a todas las empresas dado el carácter abierto que deben tener sus redes de comunicaciones y modos de trabajo. Los dispositivos de memoria externos, la comunicación por correo electrónico, la búsqueda de información en sitios web no siempre confiables, la propia ínter-conexión entre los ordenadores en la red local, son todos ejemplos de vías de entrada de software mal intencionado y son difícilmente evitables pues una compañía no siempre puede prescindir de ellos y debe buscar soluciones para asegurarlos.

Debido a este panorama, los esfuerzos en disponer de políticas de seguridad en las TIC en la gran empresa se ha disparado en los últimos años con respecto a otros tipos de compañías. En una sociedad globalizada la gran empresa debe establecer controles avanzados para asegurar la integridad, confidencialidad y disponibilidad de sus sistemas y conseguir la tranquilidad del cliente o usuario en su relación con ellas.

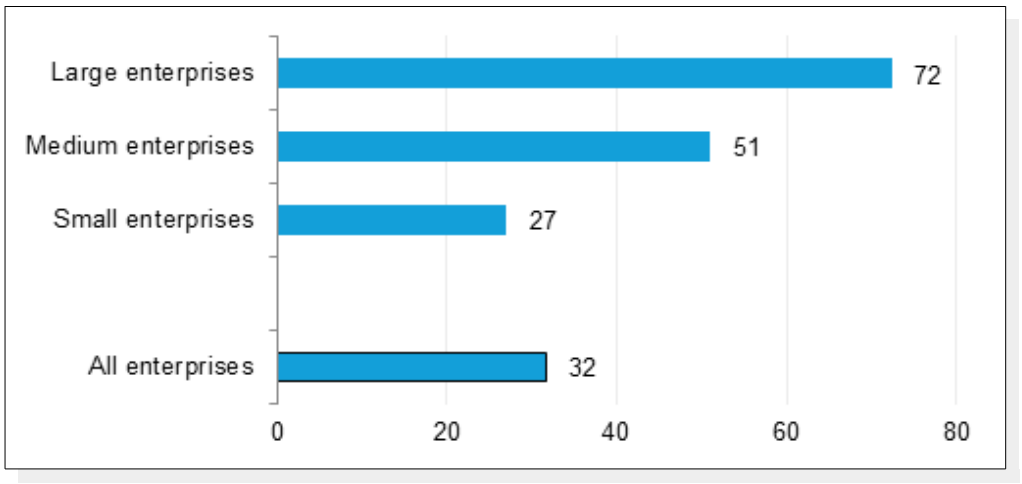


Ilustración 1: Porcentaje según tipo de empresa con política de seguridad TIC, eurostat 2016

La investigación en sistemas de seguridad para cualquier empresa esta justificada, pero hoy en día los mayores esfuerzos se están realizando en la gran empresa, motivo por el cual el presente documento trata una solución adaptable a estos entornos.

2.2. Formulación del problema

Usualmente los esfuerzos en las grandes compañías ha sido asegurar los centros de proceso de datos y sus comunicaciones. Sin embargo resulta evidente que el último elemento, el puesto de usuario, aunque no ha tenido el mismo peso en importancia como elemento individual reemplazable fácilmente que es, ha puesto recientemente en jaque a muchas empresas en ataques dirigidos a estos equipos cuando la afectación ha sido generalizada.

El empleo de políticas de seguridad en los puestos de usuario que incluyan el mantenimiento de antivirus locales sin soluciones centralizadas, genera un problema en cuanto a su desarrollo y mantenimiento. No podemos establecer mecanismos autónomos por puesto de usuario en compañías que tienen una alta dispersión de los puestos de trabajo y un elevado numero de ellos, cualquier plan de contingencia no sería posible si

precisa actuar de modo local en cada equipo, por ello se debe tratar este escenario como un problema que en sí precisa una solución especifica.

Recientemente, durante el año 2017, se han producido ataques por virus a grandes compañías, estos ataques solo han afectado los equipos informáticos de los trabajadores, sin afectar a la prestación de servicios, ni a la operativa de las redes, ni al usuario de dichos servicios (INCIBE, 2017, nota de prensa), sin embargo esta situación provoco que grandes empresas, como Telefónica, se vieran gravemente afectadas en su funcionamiento.

3. Objetivos principales

Los objetivos principales, respectos a un sistema de seguridad central de antivirus, son:

- Articular mecanismos que nos permitan poder responder de forma centralizada ante las posibles amenazas en puestos remotos evitando desplazamientos.
- Monitorización de los equipos para saber que ocurre en cada momento.
- Centralizar tareas de despliegue y actualización a lo largo del tiempo.
- Reportes de estado y de cumplimiento.
- Control de licencias y ahorro de costes.
- Optimización del ancho de banda disponible.

3.1. Resultados posibles

Cualquier empresa debería disponer de planes de seguridad. Estos planes debe cubrir múltiples apartados, nos solo en materia TIC, sin embargo el riesgo presente que suponen los ciber ataques en las organizaciones, justifican articular medidas y planes de seguridad TIC destinados específicamente a esta materia.

Como resultado posible de este proyecto, la empresa puede obtener las bases para la implementación de un plan de seguridad en lo referente a ciber seguridad, y utilizar los escenarios y riesgos cubiertos para nutrir dicha documentación.

La detección de las vulnerabilidades y las medidas tomadas para paliarlas pueden ser tomadas en gran medida de la información suministrada por la plataforma antivirus. De esta forma, en una evaluación de los riesgos, se dispondrá como uno de los referente los

virus informáticos (en cualquier de sus modalidades) y se podrá indicar el porcentajes de activos susceptibles de proteger, así como el plan de actuación y de contingencia en caso de no poder paliarlo, por ejemplo si aun no estuviera una actualización de la firma antivirus a tiempo.

4. Planificación

4.1. Enfoque del trabajo

Dado que la seguridad es un proceso, no un producto, este proyecto deberá fijar un escenario donde sea posible la gestión de la seguridad desde un sistema antivirus.

Esto nos genera dos partes diferenciadas:

- Una fase inicial de estudio del arte, que incluía un estudio de las amenazas a las que debe de responder el producto, junto con la propuesta que materializa la solución para este proyecto y marca los requisitos y lineas generales de implantación.
- Una segunda fase donde se realizara la personalización del producto en un ámbito determinado, junto con su desempeño y mantenimiento. Esta fase incluye toda la explotación del sistema, desde la definición de políticas hasta la gestión de su efectividad mediante el uso de reportes y listado de estado.

Los recursos materiales serán facilitados, el proyecto no conlleva la instalación de la infraestructura, se cuenta con ella y se centrara en el desempeño de la herramienta, su parametrización y rendimiento.

4.2. Diagrama Gantt

Desarrollamos el siguiente diagrama de planificación del trabajo.

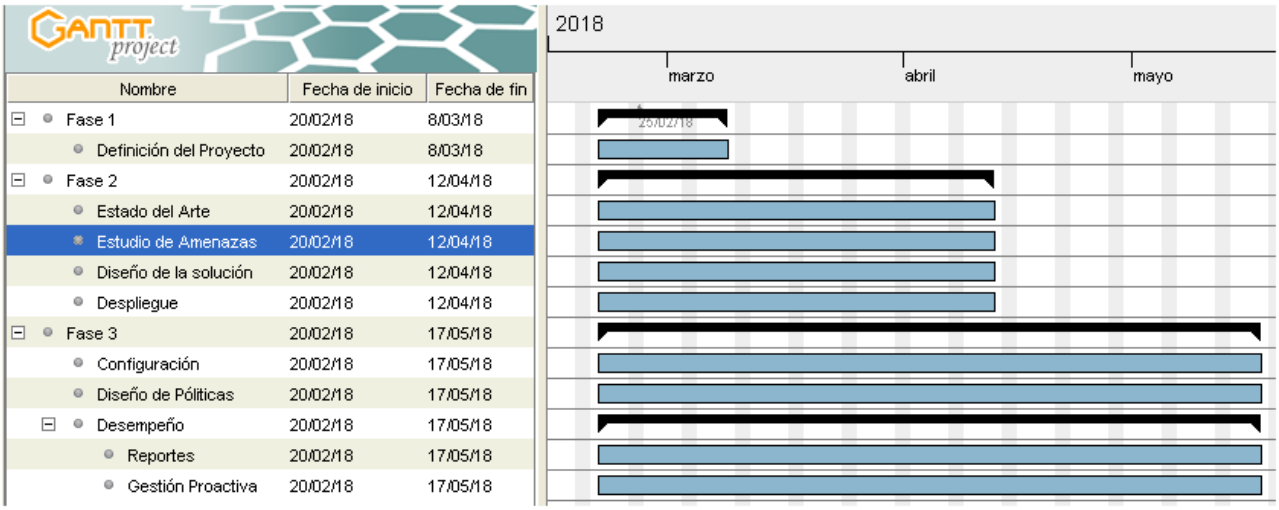


Ilustración 2: Diagrama Gant

Entregables	Definición
Estado del arte	Estudio y análisis de mercado
Estudio de amenazas	Pormenorización de los ataques mas comunes en la actualidad y los frentes que deben ser cubiertos por la solución.
Diseño de la solución	Esquema de la solución utilizada en escenarios Enterprise.
Despliegue	Aprovisionamiento de los distintos clientes antivirus e Introducción a los métodos de despliegue de forma desatendida y centralizada
Configuración	Esquema de configuración de la solución. Mediante la consola central permite realizar el diseño de la solución y establecer una alta granuladidad respecto a las distintas configuraciones y a los equipos afectados por ellas.
Diseño de políticas	Producto de mayor peso en el proyecto, dado que comporta directamente en el funcionamiento de la solución respecto a las amenazas existentes.
Desempeño	Guías para realizar el seguimiento de la solución de forma activa y medios disponibles para establecer una proactividad en el entorno de la seguridad.

Tabla 1: Entregables

5. Estado del Arte

Actualmente se dispone de dispone de distintas plataformas antivirus centralizadas EPP (Endpoint Protection Platform). Las principales diferencias entre los distintos productos viene acompañada de las funciones adicionales implementadas distintas de la propia protección antivirus en sí. Por ejemplo debemos encontrar las siguientes funciones como referencias:

- Firewall Personal
- Control de puertos y dispositivos
- Anti-malware

Es decir, no solo se deben de centran en la eliminación de procesos marcados como virus, sino que incorporan herramientas para pro-activamente evitar vías de entradas.

Vemos en el siguiente gráfico la tendencia actual de productos y su proyección en el mercado:

Ilustración 3: Magic Quadrant Gartner 2018 for EPP

Los aspectos principales que deben determinar en que punto cada uno de estos productos se pueden adaptar al entorno en el cual desplegar su solución, se debe tener en cuenta distintos apartados, algunos objetivamente técnicos y otros que complementan el producto y le aportan diferencias frente a los competidores, estas cuestiones son principalmente las siguientes:

- Eficacia ante malware: Debe controlar todo el ciclo de seguridad de este apartado, teniendo en cuenta que un punto fuerte puede ser no solo la detección sino la ayuda a la hora de recuperar la situación frente a un incidente, como por ejemplo con herramientas de restauración de la información.
- Usabilidad: En función del tipo o tamaño de la organización, puede ser recomendable una solución EPP sencilla de manejar, aunque no aporte un nivel de personalización alto, o bien una herramienta compleja que pueda ser acoplada al entorno por el equipo de TI de la organización.
- Servicios aportados: La propia funcionalidad antivirus puede que sea solo una herramienta de las iniciales que se puedan precisar, por lo tanto servicios suplementarios en la suite o bien que puedan ser incorporados a futuro pueden decantar la elección del producto, por ejemplo integración de un EDR (Endpoint Detection and Response Solutions).
- Soporte y servicio: Elementos como puedan ser el horario de soporte del proveedor del EPP o incluso el lenguaje usado, pueden determinar si el cliente encontrara un soporte adaptado a su entorno o no. Así, una compañía con servicio 24x7 deben procurar encontrar proveedores de EPP con servicios de soporte mas completos.
- Estrategia del vendedor: En este apartado entraran las distintas opciones de precio del producto con respecto a la oferta en el mercado, así vendedores de EPP que tengan en su cartera de productos otras soluciones, como por ejemplo herramientas de distribución de software, podrán ofertar paquetes de productos a un precio mas competitivo que comprados a distintos proveedores, o bien empresas que por politica busquen software con licencia gratuita.

Por la gran amplitud de actores en el mercado y diferenciación de soluciones, tan solo se realiza un análisis de la principal característica a cubrir y una muestra de los distintos productos en su desarrollo de dicho cometido: la detección y prevención de software malicioso.

Para la referencia de las pruebas se toman muestras de organizaciones independientes especializadas en pruebas de rendimiento y seguridad de productos, como es AV-Comparatives.

5.1. Detección y prevención de Malware

Aunque un EPP incluye muchas funcionalidades, la mas fundamental es la colección de características técnicas de prevención de software malicioso. Una breve clasificación de este software malicioso puede ser:

- Virus informático: Es el tipo de malware mas antiguo en definición, y su objetivo es alterar el correcto funcionamiento de un equipo y su software, normalmente archivos ejecutables. Precisa la intervención inicial de un usuario o servicio para su ejecución inicial, y una vez se realiza establece mecanismos de replicación locales (a lo largo de todos los ficheros ejecutables del equipo) y remotas, a la vez que provoca la afectación al sistema anfitrión.
- Gusanos: No precisan intervención del usuario ni la modificación de ningún fichero para infectar un equipo. Su principal misión es replicarse, lo realiza de forma autónoma por ejemplo a través de la red local de la compañía o bien con envíos de replicas a nuestros contactos de correo, y funcionar como un proceso botnet, es decir quedar en estado resilente hasta que un proceso centralizado les envíe las instrucciones a realizar en un momento particular, por ejemplo envío de correo spam, o participar en ataques DDoS (distribuidos de denegación de servicio).
- Troyanos: Software no destructivo de nuestra información ni de las funcionalidades de nuestras aplicaciones, modifica programas conocidos y añade funciones adicionales a ellos, principalmente la apertura de puertos para permitir la entrada de otro tipo de software malware. La distribución de software ilegal es el principal medio de replicación.
- Spyware: Su instalación se realiza principalmente mediante la interacción con otra aplicación no confiable, la cual genera procesos ocultos para el usuario cuya misión es la de recopilar información sobre el usuario sin su consentimiento, por ejemplo monitorizando y recopilando las acciones realizadas, para un uso posterior de esta información.
- Ad-Ware: Existe distinta controversia frente a este tipo de software, dado su finalidad es abrir ventanas emergentes o insertalas en una web conocida, mostrando publicidad en ellas mientras el usuario navega por Internet. Existe muchos organismos legales se benefician de su uso al proporcionar un medio de

publicidad selectivo y discriminatorio a sus potenciales clientes, en cualquier caso cualquier software que permita la posibilidad de poder elegir el mantenerlos o no, generara mayor libertar y control al usuario.

- Ransomware: Software malicioso cuya finalidad es provocar un secuestro de los datos alojados en el equipo infectado. Es secuestro se realiza mediante técnicas de encriptación asimétricas, las cuales utilizan una clave publica para el cifrado de los datos, pero solicitan un pago o rescate para facilitar la clave privada de descifrado. Este software se suele apoyar en otro tipos de malware para su distribución, como son los troyanos o gusanos.

Una vez clasificado el principal tipo de software del cual debe proteger el EPP a la compañía, podemos realizar un análisis comparativo, de los principales EPP, valorando su respuesta de defensa frente a ellos.

Dada la amplia heterogeneidad respecto a los modos de funcionamiento y finalidad de los distintos malware, los antivirus han debido adaptarse comprobando no solo contra una firma de antivirus local, sino también a revisar el comportamiento de los distintos programas ejecutados y en función de su sus tareas reconocer un uso perjudicial o incluso alertar al usuario para que él tome su decisión frente al mismo. Esto tiene el inconveniente que muchos malware no puedan ser detectados hasta su ejecución y puedan pasar desapercibidos en nuestro sistema de ficheros sin ser detectados o por contra generar falsas alarmas que el usuario puedo no saber interpretar, esto último será algo que penalice bastante en contra de la solución propuesta.

Finalmente la conexión a Internet también provoca distinción durante la muestra, dado que los recientes antivirus ya usan técnicas de cloud computing para la consulta de información relevante durante su ejecución, por lo que las pruebas de test se deben realizar en estado on-line y offline.

Una muestra de estos test los vemos reflejados en la siguiente tabla:

	OFFLINE Detection Rate	ONLINE Detection Rate	ONLINE Protection Rate	False Alarms
Adaware	99.7%		99.89%	2
Avast	98.8%	99.8%	99.97%	20
AVG	98.8%	99.8%	99.97%	20
AVIRA	98.0%	99.9%	99.98%	2
Bitdefender	99.7%		99.95%	2
BullGuard	99.7%		99.97%	3
CrowdStrike	93.4%		99.67%	125
Emsisoft	99.7%		99.83%	4
eScan	99.7%		99.97%	2
ESET	99.7%		99.70%	0
Fortinet	99.1%		99.35%	4
F-Secure	99.7%	99.8%	99.93%	6
Kaspersky Lab	96.0%	99.9%	99.98%	4
McAfee	78.8%	99.4%	99.62%	9
Microsoft	98.2%	99.4%	99.64%	0
Panda	65.6%	99.6%	99.98%	1
Seqrite	99.7%		99.89%	3
Symantec	86.8%	99.8%	99.89%	96
Tencent	99.7%		99.94%	3
Trend Micro	63.7%	98.6%	100%	29
VIPRE	99.7%		99.96%	3

Tabla 2: Indice de detección de Malware, fuente: AV-Comparatives, 2017, Malware Protection Test

AV-Comparatives otorga en función de distintas pruebas de detección, protección, falsos positivos, etc, una posible referencia en función de su desempeño. Se muestra a continuación:

Niveles de protección	Compañías
Advanced ++	Avast, AVG, Emsisoft, BullGuard, Kaspersky Lab, Bitdefender, VIPRE, Seqrite, eScan, ESET, McAfee, Adaware
Advanced	Panda, Tencent, AVIRA, F-Secure
Estándar	Trend Micro, Fortinet

Tabla 3: Ranking de productos EPP frente a malware

Nivel de Rendimiento	Compañías
Advanced +	Avast, AVG, AVIRA, Bitdefender, BullGuard, eScan, ESET, F-Secure, Kaspersky Lab, McAfee, Panda, Seqrite, Symantec, VIPRE
Advanced	Crowdstrike, Emisoft, Fortinet, Tencent, Trend Micro
Estándar	Adaware, Microsoft

Tabla 4: Ranking de rendimiento de productos EPP

En el comienzo de este capitulo se destacaron distintas opciones generales a la hora de la toma de elección del producto EPP, y se ha realizado también una comparación real entre distintos productos frente a un tipo de amenaza como pueda ser el malware, pero como conclusión del estado del arte actual se debe recalcar que cada organización en particular deberá revisar la solución propuesta frente a sus problemas específicos, por ejemplo, algunos fabricantes cuentan con soluciones antivirus para plataformas virtualizadas, pero si la compañía no usa esta tecnología esto no supondrá ningún aporte, en otros casos el parque de equipos puede ser muy antiguo o por contra muy actualizado (mayoría de licencias de windows XP o bien de windows 10) por lo que el producto del fabricante elegido debe estar diseñado para nuestro entorno, por lo tanto no existe siempre el producto líder para todos los escenarios posibles, aunque la aportación de este estudio pueda aportar garantías de desempeño generales en cualquiera de ellos.

6. Riesgos del proyecto.

Se establecen los riesgos de un proyecto de este tipo, lo cuales pueden afectar no solo a cuestiones meramente tecnológicas, sino a apartados como como la dedicación, desde el punto de vista de los recursos humanos disponibles, u organizativas como son la afectación dentro de los distintos workflow ya establecidos en la propia Compañía.

6.1. Riesgos tecnológicos

La nueva visión de amenazas, que hasta la implantación de la herramienta pudieran ser desconocidas, y las acciones que se determinen para la remediación de las mismas,

puede precisar adaptar lineas de trabajo ya existentes y consolidadas, dentro de estas líneas de trabajo se sitúan:

- Maquetación de equipos
- Despliegue de parches de seguridad.

Se deben tener en cuenta que los riesgos detectados se corresponden con malware, en cualquiera de las variantes ya mencionadas en uno de los capítulos de este proyecto, si bien en muchos casos la propagación de los mismos esta hoy en día muy relacionada con la explotación de agujeros de seguridad detectados en software de terceros ya consolidados en el mercado, como pueda ser software ofimático, de animación, lectores de documentos, etc.

Es por tanto que las lineas de trabajo establecidas respecto a la maquetación y al despliegue de parches de seguridad, corrección de errores y vulnerabilidades esta íntimamente ligado a los procesos de remediación y aplicación de un software antivirus.

En la maquetación de equipos tendremos que incluir los siguientes aspectos generales:

- Instalación de agente antivirus.
- Instalación de sistema de despliegue de actualizaciones.

Para el despliegue de actualizaciones, contamos en el mercado con distintas soluciones, es clave para un proyecto de este tipo cubrir este riesgo e implantar en la Compañía la solución que pueda ser utilizada en todos los escenarios posibles.

Podemos indicar las siguientes vías de despliegue:

- Consola centralizada

  En este apartado podemos incluir herramientas de terceros que integran un agente en cada equipo cliente, un servidor que gestiona los clientes, y un repositorio de información. Dentro de este tipo de software encontramos soluciones como Cliente Management Suite de Symantec, OCS Inventory, etc

- Gestión por Directorio

  En Compañías con un alto numero de equipos, es habitual disponer de servicios de Directorio, basados en LDAP o propietarios. Dentro de las herramientas de gestión

que incluyen estos esquemas, es posible introducir políticas de despliegue de software, por ejemplo usando GPO en Directorio Activo de Microsoft.

Dentro de los riesgos tecnológicos, también se debe controlar el impacto que el conjunto de soluciones de antivirus pueden provocar en la red de la Compañía, así es preciso conocer la arquitectura actual, evaluar los puntos críticos de las redes de telecomunicación, y diseñar medidas que permita el despliegue de la solución sin un impacto alto en el trafico de datos. Para ello se deben determinar nodos intermedios encargados de distribuir el software en redes comunicadas mediante líneas WAN con los sistemas centrales antivirus.

6.2. Riesgos organizativos

Un proyecto de antivirus requiere un proceso de maduración de la Organización en esta línea y una especialización y división del trabajo.

Actualmente podemos indicar que existen distintas metodologías para la gestión y manejo de los procesos de IT en una Compañía, y con ellos poder, entre otros objetivos, implementar controles y medidas que puedan ayudar a mitigar los riesgos intrínsecos a los sistemas de información. Podemos indicar principalmente: ITIL, CobIT o ISO 27001.

La gestión o gobernanza mediante cualquier sistema de gestión nombrado, implica un impacto respecto al servicio de soporte de la Compañía, conocido como Service Desk, el cual deberá ser manejado y articulado de forma que no provoque un impacto en la compañía.

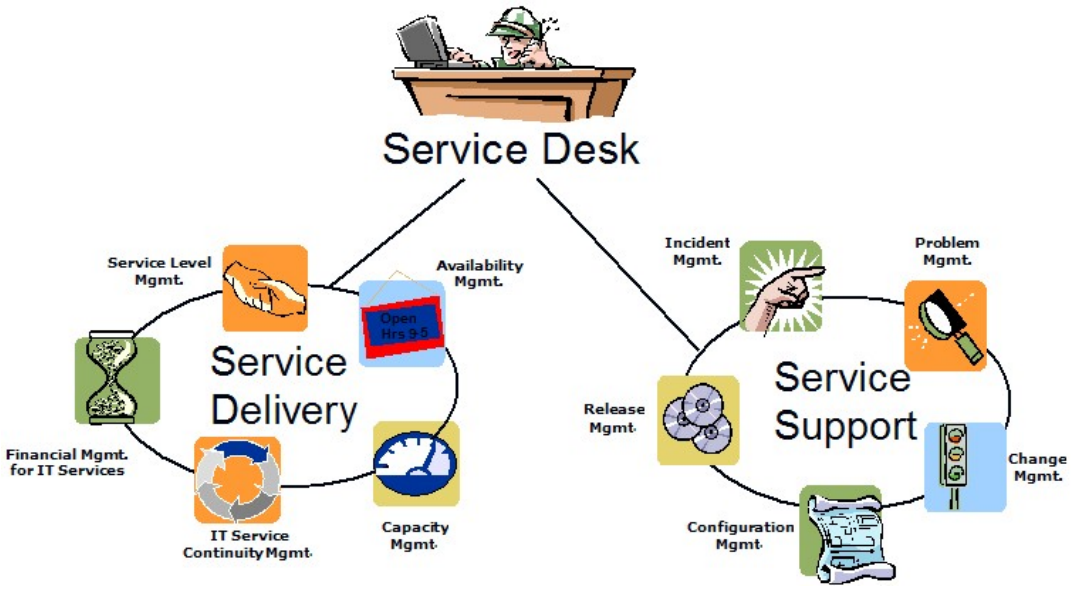


Ilustración 4: Procesos de ITIL

Sin entrar en las particularidades de estos modelos de gestión, ni en su implantación en una Compañía, lo cual no es objeto de este proyecto, si podemos indicar que establecerá líneas de trabajo en la llamada “Gestión de la Seguridad de la Información”, y que esta gestión de la Seguridad será un proceso cíclico, obteniendo resultados intermedios y retroalimentandose en función de las mejoras introducidas paulatinamente. La Seguridad es entendida de esta forma como un servicio y no como un producto.

Para la gestión de la Seguridad, en lo referente al sistema antivirus, podemos introducir las siguientes medidas y/o una combinación de ambas:

- Ampliar funcionalidades de los departamentos de IT actuales
- Generar grupo especializado en Seguridad

Las funcionalidades a introducir en dichos grupos de trabajos se pueden enumerar en las siguientes:

- Gestión del nivel del servicio antivirus.

  Definición del nivel del servicio de antivirus, el cual se adaptara al entorno de trabajo de la Compañía, estableciendo componentes operativos, firewall, IPS, etc.

- Implementación de Medidas y controles de seguridad

  Definición de controles de seguridad, niveles de protección requeridos y sus actualizaciones, así como medidas de registro de detecciones.

- Mantenimiento del sistema

  Procedimientos de actuación por parte de los distintos niveles de soporte de IT y actuación para solventar los daños producidos en los equipos.

- Modificación del sistemas

  Propuestas de mejoras en políticas aplicadas y modificación de niveles de seguridad.

Estos apartados modificaran el Workflow de operación implantado en la Compañía, generado un proceso cíclico en el cual cada fase alimenta procesos de las áreas de actuación.

El mayor riesgo en la no aplicación de un protocolo de Seguridad Antivirus, puede provocar que el antivirus se convierta en un producto, el cual una vez implantado no se mantenga, considerando que las actualizaciones automáticas, y la autonomía del motor del antivirus proporcionen por si solos los resultados y generando una falsa sensación de seguridad respecto al estado real de la Seguridad en la Organización.

7. Entorno de implantación del proyecto.

El proyecto se desarrolla en un entorno sanitario de ámbito provincial, formado por distintos centros de trabajo, con una envergadura y criticidad distinta entre ellos, y comunicados todos ellos por una red corporativa privada.

Los centros están compuestos por:

- Hospitales

  Los Hospitales son centros donde confluyen un gran numero de profesionales, y cuya disponibilidad es total, 24x7x365, en determinadas zonas de trabajo. Los Hospitales de referencia son:

- Hospital Universitario Virgen del Rocío
- Hospital Universitario Virgen Macarena
- Hospital Virgen de Valme
- Hospital de Osuna

- Distritos Sanitarios.

  Los Distritos Sanitarios son centros de gestión, donde no se presta atención sanitaria directa y sirven de soporte para los centros de atención primaria. Se dispone de los siguientes Distritos:

  - Distrito Sanitario Sevilla Norte
  - Distrito Sanitario Sevilla
  - Distrito Sanitario Aljarafe

Se indica una representación de esta Organización de forma gráfica:

Ilustración 5: Distribución por centros

Esta Organización forma parte del Servicio Andaluz de Salud en la comunidad autónoma de Andalucía, en la cual sus centros son financiados por fondos públicos los cuales

proporcionan también determinados acuerdos de servicio realizados con empresas proveedoras.

Uno de los acuerdos establecidos se ha realizado con la empresa Symantec, corporación estadounidense que desarrolla y comercializa software de gestión de para activos de TI y seguridad informática. Bajo este acuerdo es posible utilizar distintas herramientas y componentes, como por ejemplo el software de gestión de puestos de trabajo llamado Client Management Suite o CMS (Symantec, 2017, Product Catalog), el cual permite disponer de una base de datos con información de todos los activos instalados en una Compañía e interactuar con ellos mediante un agente de comunicación, que puede realizar tareas desatendidas sobre ellos como son el despliegue y control de software instalado.

Adicionalmente también se dispone en la Organización de un servicio de Directorio Activo de Microsoft, el cual gestiona las credenciales de usuarios y cuentas de equipos de toda la organización, facilitando un inicio de sesión en cualquier ordenador de la Organización

En el aspecto funcional y respecto a cuestiones de operación en el ámbito de las TI, la Organización cuenta con los siguientes agentes:

Denominación	Disponibilidad	Funciones
Call Center	24x7x365	Registro de incidencias
Soporte Puesto a Usuario	24x7x365	Soporte básico de primer nivel
Atención Especializada nivel 2	24x7x365	Soporte especializado y de apoyo al primer nivel
Soporte funcional	Horario laboral	Soporte funcional de aplicaciones

Tabla 5: Elementos funcionales del proyecto

Salvo el “Soporte funcional”, todas estas funciones se encuentran dentro de un acuerdo de servicio con terceras empresas independientes a la Organización.

8. Propuesta

Para esta propuesta vamos a tomar el producto EPP de Symantec llamado SEPM. Dicha compañía, situada entre las líderes de este sector, aportan también un amplio porfolio de soluciones en distintos ámbitos complementarios al propio EPP, como pueda ser por ejemplo herramientas para el control del parque de dispositivos, con soluciones como su Altiris ASM (Asset Management Suite) (Symantec, 2017, Catalogo de Productos). Estas posibilidades de ampliación, que afectan a la estrategia de compra, aportar a la vez uno de los entornos de administración mas comprensivos pero que igualmente incorpora herramientas avanzadas de protección y detección, y finalmente un buen nivel de servicio de soporte en jornadas de 24x7 (AV-Comparatives, 2016, Support Test) complementan los requisitos acordes a un entorno de gran compañía, y se encuentran entre los aspectos principales indicados en el capitulo anterior y que deben marcar el punto de partida en cualquier elección realizada. A esta justificación del propio producto, se añade que el producto esta disponible para la Organización gracias al acuerdo disponible para el Servicio Andaluz de Salud, por lo cual se posiciona en una situación estratégica por encima del resto de compañías, proporcionando ademas un producto que ha sido analizado como optimo para este desarrollo.

8.1. Convenciones y terminología

Las siguientes convenciones y terminología son usadas en este documento:

Convenciones	Terminología
SEP	Symantec Endpoint Protection
SEPM / SEP Manager	Servidor de gestión de SEP, proporcionando consola web o Java
GUP	Group Update Provider
CPD	Centro de Proceso de Datos
Heartbeat	Intervalo de tiempo entre conexiones del cliente SEP al servidor SEPM
Site	Organización de servidores SEPM que se conectan a una misma base de datos.

Tabla 6: Terminología del proyecto

8.2. Componentes del producto antivirus

a) Básicos

Los componentes principales y mínimos con los que cuenta dicho producto son:

- SEPM (Symantec EndPoint Protection Manager)

  Este elemento es el núcleo principal del producto, en él se encuentran los elementos fundamentales para su despliegue, como son el motor de base de datos, que puede estar soportada por un servidor SQL Server de la compañia, y el propio software servidor de administración que ofrece los servicios hacía los clientes e integra la propia consola de gestión. Desde esta consola se realizan las funciones principales de gestión y administración como son:

  - Gestionar el inventario de los clientes SEP desplegados en la plataforma.
  - Administrar de forma centralizada las configuraciones y políticas aplicadas a los clientes SEP sobre los que tiene autoridad.
  - Mantener una comunicación periódica con los clientes SEP para monitorizar el “estado de salud” del software cliente antivirus.
  - Descargar actualizaciones de contenido (firmas antivirus, etc.) y de producto (actualizaciones del software).
  - Distribuir las actualizaciones de contenido y de producto a los clientes SEP.
  - Recolectar información de eventos y logs de los clientes SEP gestionados.

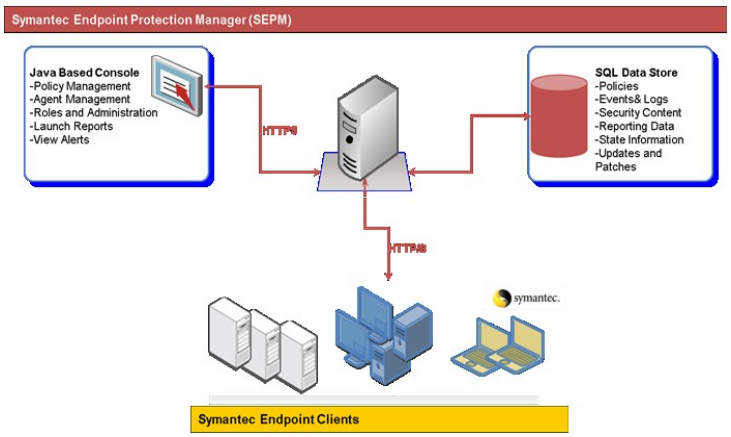


Ilustración 6: Symantec Endpoint Protection Manager

- Base de Datos

El servidor SEPM almacena información sobre políticas, configuración, clientes, contenido, eventos y logs en una base de datos. Esta base de datos puede ser integrada (Sybase Anywhere 9) o externa (Microsoft SQL Server 2000/2005/2008).

Los servidores SEPM se pueden agrupar en “Sites”, que se definen como un grupo de servidores SEPM que utilizan una misma base de datos. Los sites se pueden interconectar mediante relaciones de replicación (de contenido, de logs, o de políticas)

La arquitectura de la solución permite gran flexibilidad a la hora de configurar una solución adaptada a las necesidades funcionales, organizativas y topológicas de la organización.

- Cliente SEP (Symantec Endpoint Protection).

  Los clientes antivirus (SEP) son programas diseñados para proteger los equipos contra virus y riesgos de seguridad generados por código malicioso y que afecta a los soportes de información y redes de telecomunicación. Dependiendo de la configuración que se programe sobre dichos clientes, también se puede llegar a proteger los equipos frente a código malicioso que accede a la organización a través de archivos adjuntos de correo electrónico o mediante navegación por Internet.

  El mecanismo de funcionamiento de un cliente antivirus es el siguiente: De forma predeterminada, al arrancar el antivirus, este carga el fichero de definiciones de virus y los motores de búsqueda. En la fase de análisis, cuando se detecta un virus, como primera acción, se intenta limpiar el archivo infectado y reparar los efectos del virus. Si se consigue limpiar el archivo, el virus quedará eliminado totalmente. Si no se consigue limpiar el archivo, el cliente antivirus emprende una segunda acción, que consiste en moverlo al área de cuarentena para que la infección no se extienda. Tras poner el archivo en cuarentena el cliente antivirus trata de devolver a su estado previo la información del sistema que modificó el riesgo de seguridad. En cualquiera de los casos, los servidores de antivirus son informados sobre el riesgo detectado.

  Otra de las funciones del cliente antivirus es recibir las actualizaciones del fichero de definiciones de virus que se ofrecen desde el servidor primario de administración de la plataforma. Cuando se realizan estas actualizaciones, el cliente antivirus comprueba de forma automática si hay archivos almacenados en el área de cuarentena y ofrece la oportunidad de analizarlos empleando la nueva información de protección.

Los clientes de antivirus pueden organizarse en grupos de clientes. Esto permite agrupar los clientes que requieren niveles de acceso y configuraciones similares. Es posible configurar de forma simultánea varios clientes mediante la configuración de valores de grupo, en lugar de hacerlo de forma individual. Se pueden crear, ver y configurar los grupos de clientes desde la consola de administración.

La funcionalidad básica requerida de antivirus y antispyware puede verse complementada por funcionalidades extras como: firewall, prevención de intrusiones (reactiva y proactiva), control de aplicaciones, gestión de dispositivos del cliente, etc. Estas funcionalidades pueden ser parte integral del cliente, de forma que puedan ser activadas de forma centralizada en el momento que se considere necesario.

Cabe destacar que los clientes antivirus pueden ser instalados tanto en puestos finales de usuarios como en los servidores que lo admitan.

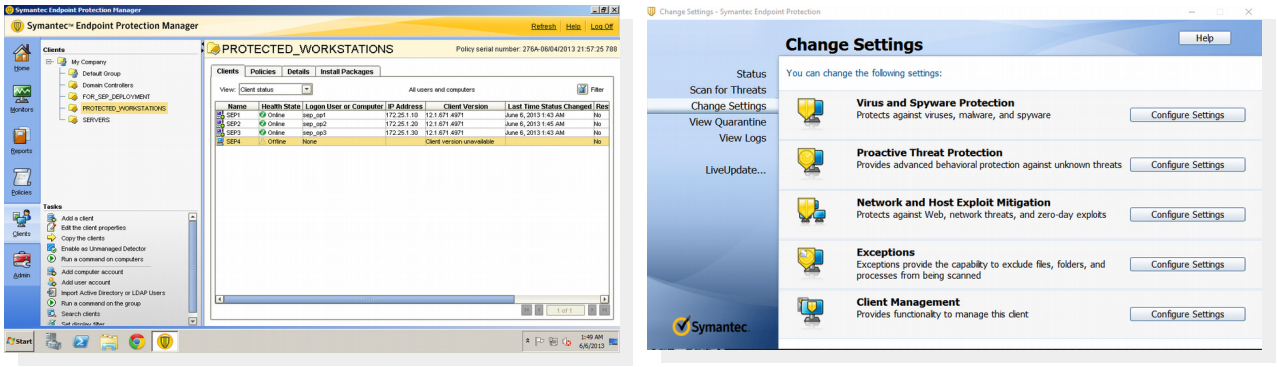


Ilustración 7 Consola SEPM y cliente SEP

b) Opcionales

Los componentes opcionales a la arquitectura antivirus de Symantec son:

- Administrador de LiveUpdate

  Centraliza la descarga de las actualizaciones de producto, como puedan ser las definiciones y firmas antivirus. De esta forma descarga al servidor SEPM de esta tarea y se puede encargar de su distribución a los clientes.

- GUP (Proveedor de actualizaciones de grupo)

Symantec Endpoint Protection permite la designación centralizada de un cliente SEP como “proxy” (GUP, o “Group Update Provider”) de actualizaciones de contenido para el grupo en el que se encuentra.

Esto permite reducir sustancialmente el ancho de banda utilizado para actualizaciones, especialmente en localizaciones geográficas remotas con limitaciones de conectividad y ancho de banda, ya que sólo el cliente designado como “proxy” es el encargado de conectarse a través de la línea al servidor SEPM correspondiente para descargar las actualizaciones. El resto de clientes del grupo las obtienen del cliente designado como “proxy”.

Es importante destacar que el “proxy” sólo sirve para distribuir actualizaciones de contenido (definiciones de firmas antivirus y reglas del sistema de protección de intrusiones), y no para actualizaciones de las aplicaciones, como se muestra en la siguiente tabla:

Función	Descripción
Comunicación cliente-servidor (heartbeat, políticas, etc.)	El cliente se conecta a los servidores SEPM definidos por orden de prioridad.
Actualizaciones de contenido	El cliente obtiene las actualizaciones de contenido preferentemente del GUP. En caso de no disponibilidad del GUP, las actualizaciones se obtienen del servidor SEPM correspondiente.
Actualizaciones de aplicación	Las actualizaciones se obtienen del servidor SEPM correspondiente.

Tabla 7: Funciones GUP

Un GUP (Group Update Provider) puede ser cualquier cliente SEP que esté disponible de forma continua y tenga direccionamiento IP estático.

- IT Analytics Server

  Su función es elaborar consultas e informes personalizados, que permiten una definición personalizada en cada entorno allí donde los informes básicos que incorpora el producto son insuficientes.

8.3. Arquitectura de la plataforma

El diseño de un producto con un arquitectura distribuida, como es un EPP, siempre supone un reto para cualquier organización, los factores que deben ser tenidos en cuenta a la hora de valorar el diseño final son entre otros:

- Las tecnologías del producto que desplegaremos y las características de los equipos.
- La unificación o no de las políticas de seguridad en los distintos clientes, y la generación de los grupos administrativos que serán precisas, por ejemplo la diferenciación por tipo de soporte (portátiles, estaciones de trabajo, etc) o bien por departamentos u otros criterios.
- Elemento clave es la distribución geográfica de la organización, junto con el volumen de clientes por sede y su tecnología de comunicación (ancho de banda, tipo de linea, etc).
- La frecuencia de las actualizaciones y parches.
- La definición de la alta disponibilidad para este servicio.

El objetivo de este proyecto es mantener esta administración distribuida pero centralizar la plataforma de SEPM a nivel provincial, donde poder unificar los criterios indicados anteriormente.

Teniendo en cuentas estas consideraciones y dado el entorno de trabajo propuesto, la arquitectura definida para el despliegue de la solución se define por los siguientes componentes: 2 servidores SEPM

Según Symantec Best Practices (2016, p. 11) para una medía de 18.000 clientes por conexión en pull mode, y 500 en push, mediante HTTP precisamos un servidor central SEPM, y para obtener tolerancia a fallos se precisán dos servidores conectados a la base de datos

Según estos datos, Symantec Endpoint Protección contará con dos consolas de administración asignadas a un mismo site, con configuración de alta disponibilidad y balanceo de carga. Ambas consolas se comunicarán con la base de datos externa que se instalará en un servidor de base de datos. Este modelo podrá dar servicio a un entorno de hasta 10.000 clientes por provincia, estimados.

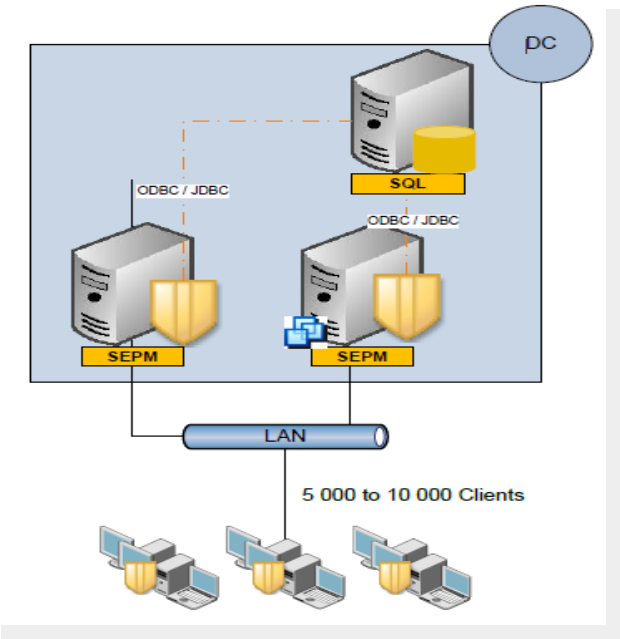


Ilustración 8: Arquitectura tolerante a fallos SEPM

En el caso de sedes con conexiones inferiores a 10Mb será obligatorio el uso de GUPS para la distribución de firmas. En cualquier otro caso siempre será recomendable el uso de GUPS por lo que se desplegaran distintos GUP que permitirán proporcionar las actualizaciones a los clientes SEP y balancear la carga de los servidores, un solo GUP puede dar servicio hasta a 10000 clientes y solo precisa un máximo de 1 GB de almacenamiento (Symantec Best Practices, 2016, p. 14).

En la metodología seguida para el diseño de la arquitectura de servidores se define la siguiente hoja de recogida de datos:

Sedes	Total equipos	Ancho de banda	Criticidad	Disponibilidad
H.U.V.R	7500	Macrolan 100 Mb	Alta	24x7
H.U.V.M	5000	Macrolan 100 Mb	Alta	24x7
H.V.V.	3000	Macrolan 100 Mb	Alta	24x7
H.O	1500	Macrolan 100 Mb	Alta	24x7
D. Aljarafe	250	Macrolan 10 Mb	Media	Laborables
D. Norte	250	Macrolan 10 Mb	Media	Laborables
D. Sevilla	250	Macrolan 10 Mb	Media	Laborables

Tabla 8: Hoja de recogida de datos

8.4. Despliegue de clientes

Para la fase de despliegue se realizan las siguientes tareas:

- Identificación de los equipos clientes

  Es preciso conocer los sistemas operativos, y características generales de los dispositivos para poder elegir las versiones de producto a desplegar, o bien la imposibilidad de ello que se pudiera encontrar en el escenario propuesto.

- Identificación de los grupos de equipos

  Los grupos de equipos se utilizan principalmente para tareas de configuración de políticas y de producto en los equipos. Puede ser necesario implementar distintas políticas en el caso por ejemplo de equipos móviles como puedan los portátiles.

Para definir el despliegue y organización se realiza un sondeo con la siguiente hoja de toma de datos:

ID Equipo	Sistema Operativo	Memoria	Almacenamiento	Criticidad	Móvilidad
SEP213	Windows XP SP3	512	150GB	Baja	NO
SEP120	Windows 7	4 GB	500 GB	Media	NO
SEP300	Windows 8.1	4 GB	500 GB	Alta	NO
SEP100	Windows 10	4 GB	1 TB	Alta	SI
SEP221	Mac OS	2 GB	500 GB	Media	SI
SEP212	Ubuntu 11	2 GB	500 GB	Media	NO

Tabla 9: Ejemplo de Hoja de recogida de especificaciones clientes

Tras el análisis de datos, detectamos una versión se sistema operativo en proceso de discontinuación de soporte por el fabricante: Windows XP. Planteamos utilizar en estos casos una versión del agente compatible con la consola central SEPM, si bien no es la última versión operativa del cliente y debemos valorar una migración de estos equipos a lo largo del tiempo. Esto nos determina utilizar las siguientes versiones de SEP:

- Versión 12.1.x : Equipos Windows XP
- Versión 14.x: Resto de equipos.

En base a estas versiones de SEP, se realiza el aprovisionamiento en la consola SEPM de los paquetes de instalación que serán necesarios para el entorno actual.

Se aprovisionan y configuran los distintos sistemas operativos:

- Windows en versiones 32 y 64 bits
- Mac OS
- Linux

Este requisito es necesario para proveer un despliegue que permita la instalación de las distintas versiones de cliente antivirus (SEP). En ello ha sido clave que el proveedor del EPP dispusiese de versiones para todos los distintos equipos desplegados en la compañía.

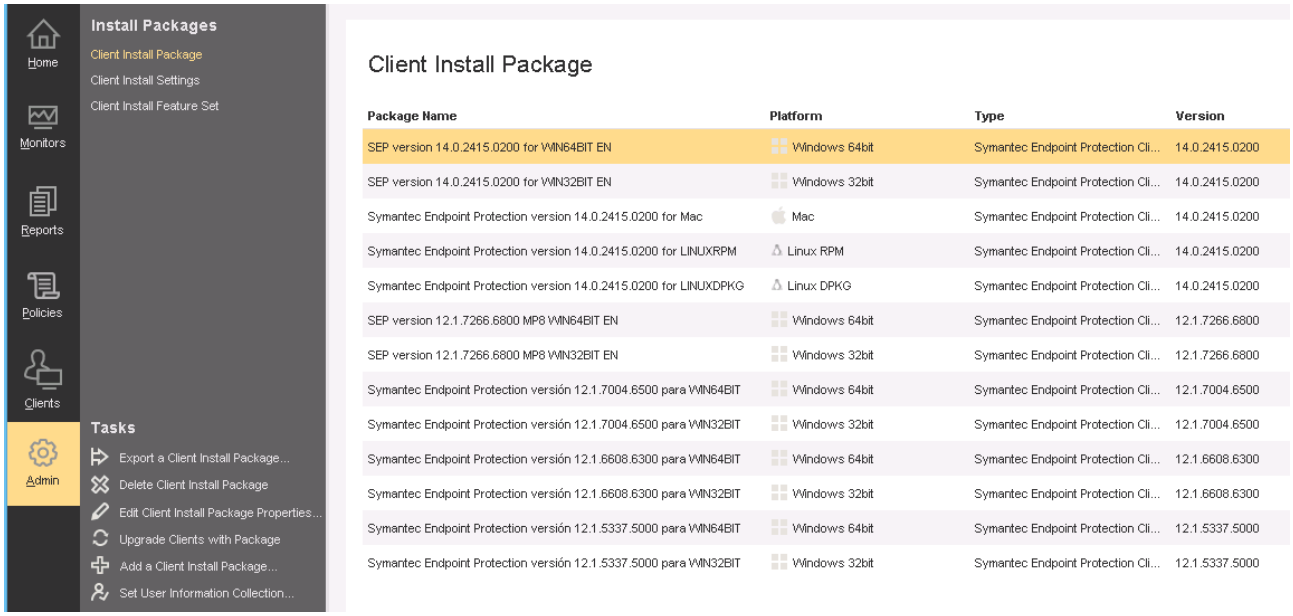


Ilustración 9: Clientes aprovisionados SEP

Se define la estructura por centros, en la cual se definen las áreas de trabajo principales, en ellas se incluirán los equipos desplegados:

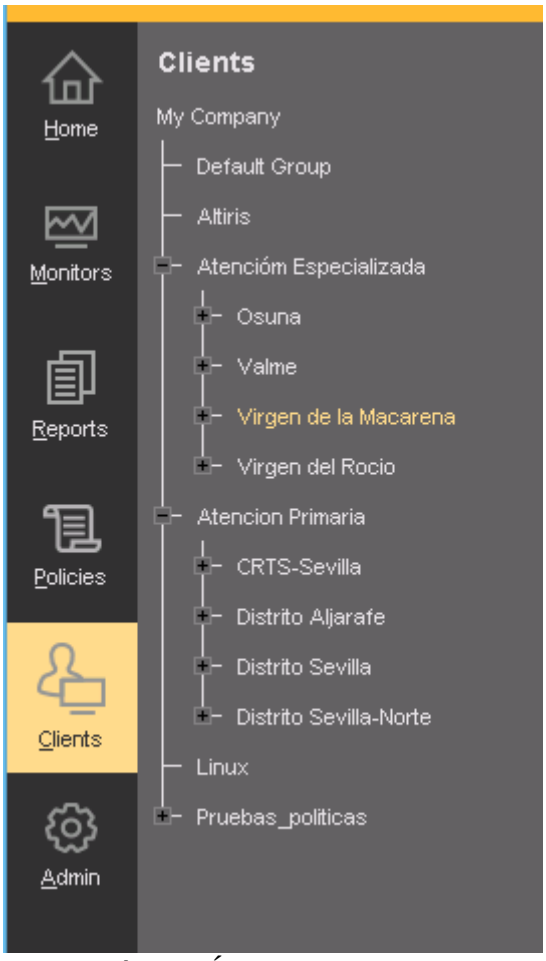


Ilustración 10: Árbol de Unidades Organizativas SEPM

La instalación en los clientes se realizara mediante 2 acciones:

- Despliegue inicial
- Mantenimiento del parque de equipos.

Para el despliegue inicial se realiza mediante la consola SEPM, para el mantenimiento del parque se utilizarán las políticas de dominio (GPOs de Directorio Activo) que agregaran el cliente a los nuevos equipos incluidos en el parque.

El despliegue inicial mediante la consola SEPM, debe tener en cuenta que usaremos el repositorio de clientes que hemos definido para la Organización. Adicionalmente, para minimizar los riesgos en el tráfico de red, se despliega el cliente con un fichero básico de

firmas: el Contenido Básico (Tiene un tamaño de 80MB para paquete básico y 500MB para el paquete completo. Siempre se recomienda hacer el sencillo y delegar la actualización de firmas a los GUPS asignados

El despliegue se realiza en el segmento de red de cada sede, siendo posible indicar el intervalo de direcciones IP o bien un fichero con la lista de equipos o el nombre de un equipo particular.

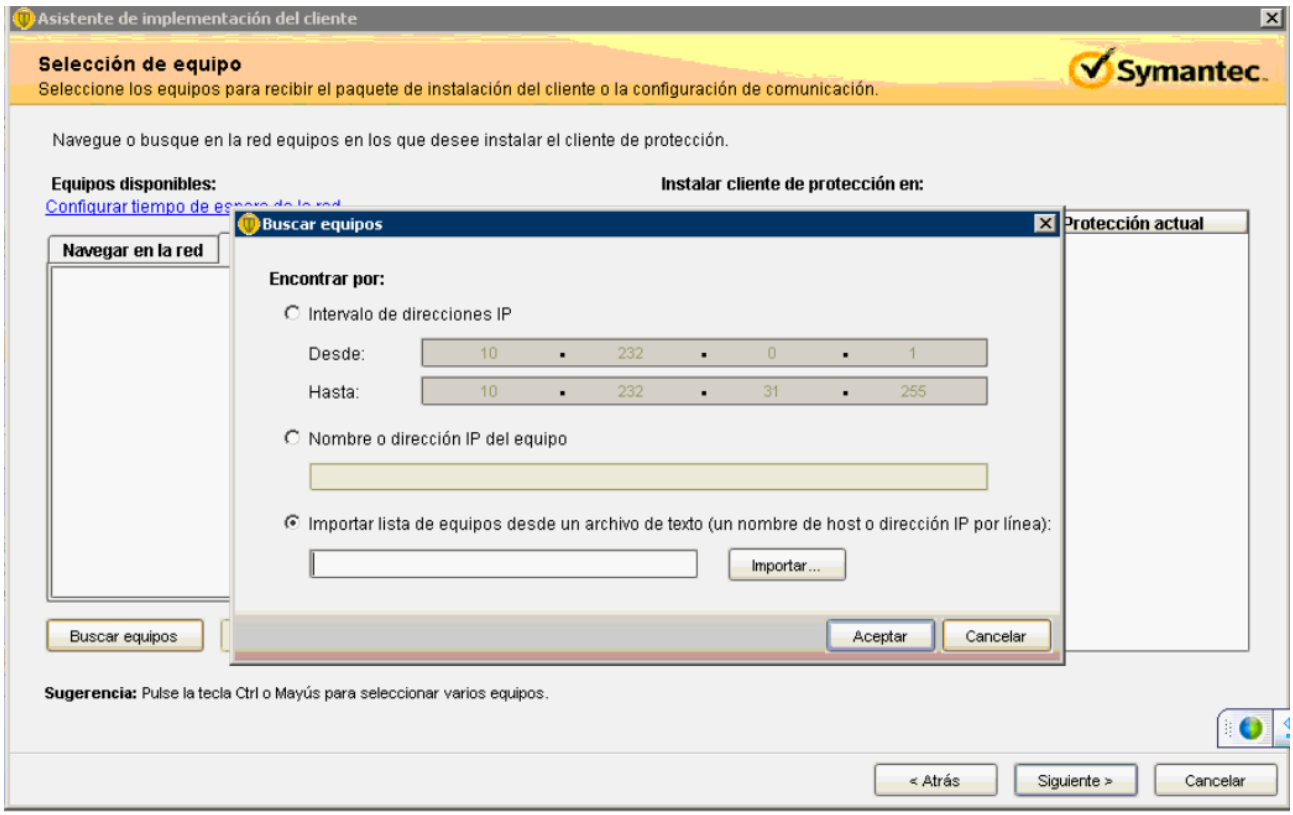


Ilustración 11: Selección de segmento de red en despliegue

Se indican una serie de recomendaciones que se deben tener en cuenta en cualquier despliegue:

- Evitar los despliegues sobre el Default Group. En caso de tener que utilizarlo retirar políticas Liveupdate de actualización. La indebida localización de clientes en este grupo puede provocar saturación y problemas en la red. Este grupo se ha de usar como área de paso.
- Revisar y estandarizar políticas y configuraciones: En esta fase del proyecto se ha optado por usar las políticas por defecto, dado que la configuración de políticas se

realiza en la siguiente fase del proyecto según el cronograma facilitado en la PEC1. Una diferencia de políticas en los distintos hospitales o centros pueden generar incoherencias a nivel de soporte. Ej: Clientes que en Hospital Macarena piden contraseña para detener servicio no lo hacen en Osuna o V. del Rocío. Desde un punto de vista administrativo se recomienda adoptar una postura única y aplicarla a cada uno de los grupos. Esto se ha de hacer estudiando minuciosamente cada uno de los casos y entre todos los administradores que harán uso de la plataforma.

8.5. Despliegue de contenido.

Los clientes antivirus son componentes que requieren una actualización continua para mantener actualizada su protección antivirus. Las principales actualizaciones que se realiza sobre ellos son los llamados “ficheros de firmas”, que es el conjunto de definiciones, del que dispone la compañía proveedora de la solución, del software determinado como malware registrado como tal en la fecha de distribución.

La solución ofrece distintas alternativas de actualización:

- SEPM: Directamente desde el servidor.
- LiveUpdate: Servidor dedicado de actualizaciones, puede ser interno en la red y la Organización o bien un servidor de Internet.
- GUP: Group Update Provider, servicio de apoyo a la distribución únicamente de firmas antivirus, políticas y nuevo software cliente antivirus no pueden ser desplegados de esta forma.
- Software de terceros: Software ajeno a la solución antivirus que puede desplegar software. Usando esta función es posible desplegar “Intelligent Updates”, que son aplicaciones distribuidas en un portal de Symantec que contienen las firmas y contenido suficiente para actualizar manualmente los clientes.

(Symantec, 2017, Método de distribución de contenido)

Dentro de la arquitectura definida en la Organización, contamos a nivel regional con un servidor de LiveUpdate, que puede ser usado provincialmente por cada Site en su definición de distribución de contenido.

En el entorno de la Organización donde se despliega esta solución, no es recomendable delegar por completo la gestión de las actualizaciones a los servidores SEPM, bien por el numero de cliente, bien por las lineas de comunicaciones de algunos centros de trabajo. Por lo que, tal como se indico en la arquitectura inicial, es preciso desplegar equipos con funciones de GUP a lo largo de las distintas sedes, es por ello que se define la siguiente distribución de contenido para el entorno provincial donde se desarrolla el proyecto:

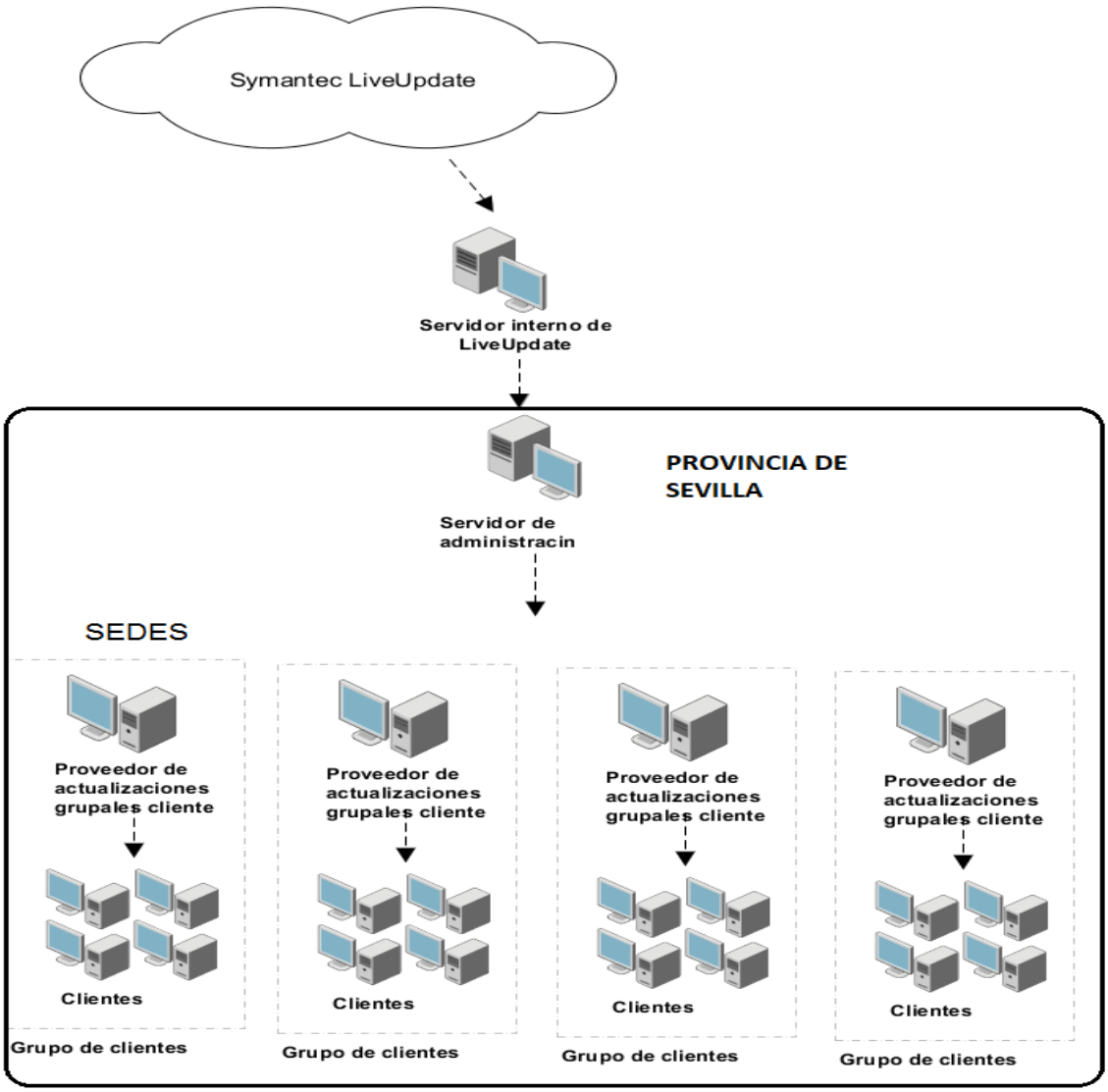


Ilustración 12: Distribución de contenido

Una vez determinados los equipos que realizaran las funciones de GUP en las sedes remotas, se debe realizar la configuración de una política de actualización en la consola SEPM.

El procedimiento a seguir es configurar una política de liveupdate para cada sede que disponga de un GUP. En dicha política se establece que mientras que el GUP este disponible se procede a realizar la petición de nuevas firmas antivirus a dicha maquina, y que en caso de no estar disponible se usara el servidor regional LiveUpdate, de esta forma se evita la consulta directamente contra Internet de un servidor LiveUpdate de Symantec a la vez que se libera de esta carga a los servidores SEPM del site.

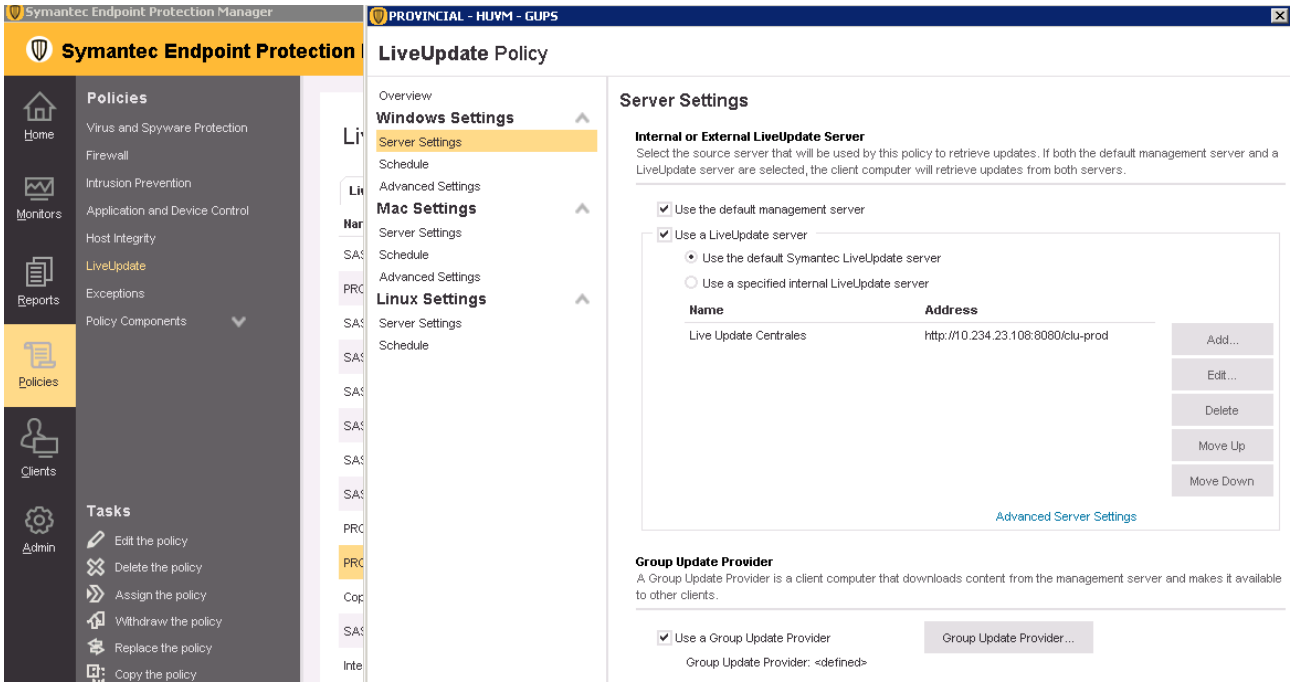


Ilustración 13: Política de despliegue de contenido

En la configuración detallada del GUP, se selecciona la maquina o grupo de maquinas que realizaran dicha función, así como valores de seguridad como son el espacio de tiempo en el cual el cliente tratara de contactar con el GUP antes de saltar al servidor LiveUpdate, periodo de retenciones de firmas, puertos de escucha y numero de clientes simultáneos.

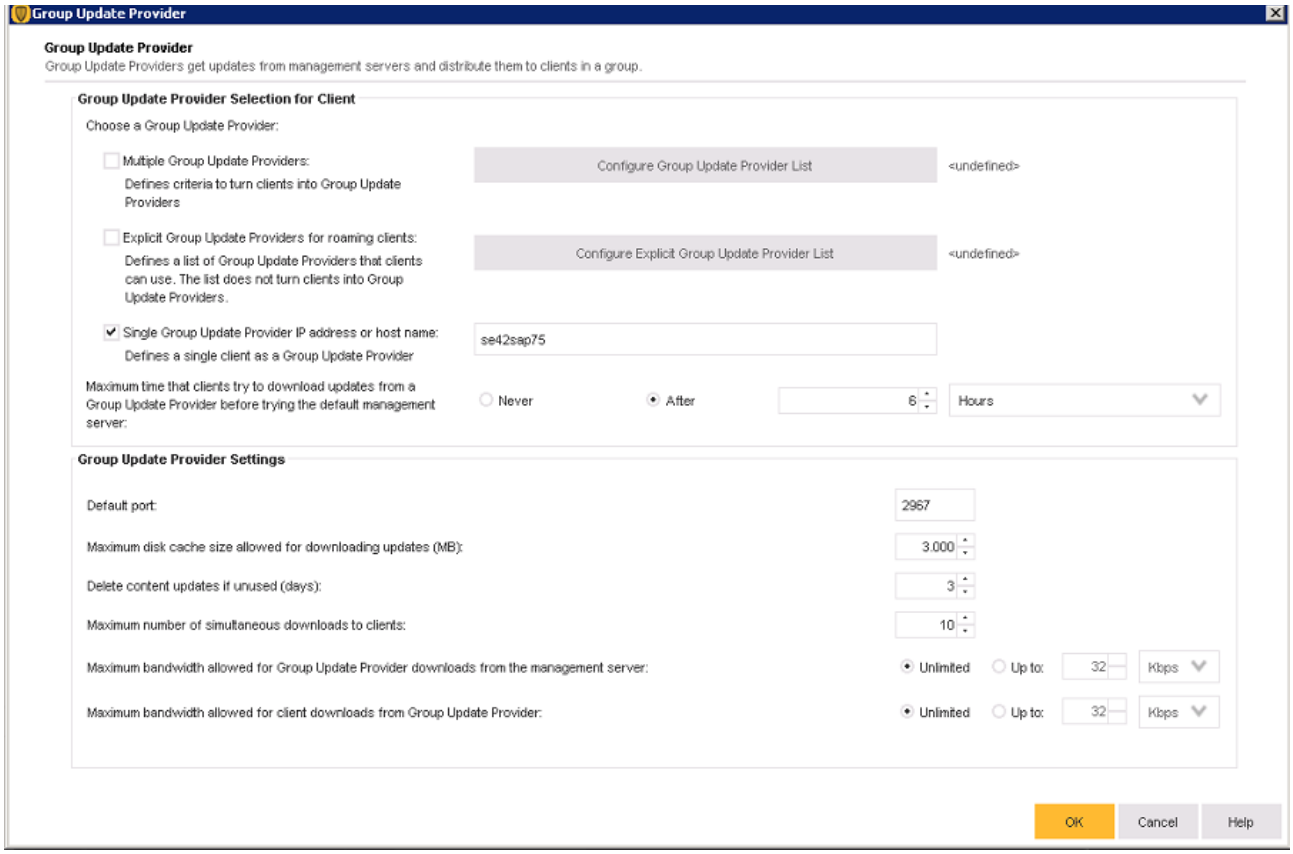


Ilustración 14: Configuración de GUP

Para esta configuración es importante tener en cuenta la periodicidad con la cual el fabricante libera nuevas versiones de firmas, así como la disponibilidad de los equipos clientes.

El fabricante, Symantec, libera 3 veces al día nuevas firmas (Symante, 2016, actualización definiciones de virus), esta frecuencia es importante para poder dar respuesta a las amenazas de día cero.

Los equipos de la compañía son usados como media en jornadas de 7 horas diarias, en algunos puestos de trabajo puede variar la disponibilidad y el uso diario dado que tratamos entornos con una alta disponibilidad como son los centros sanitarios.

Con estos valores se define que el periodo de consulta de actualizaciones al GUP no puede ser superior a 7 horas, de forma que, en la jornada laboral, los clientes siempre tengan margen de consultar a su servidor de LiveUpdate regional y obtener su actualización diaria. Es por ello que se configura un tiempo máximo a 6 horas de disponibilidad del servicio GUP.

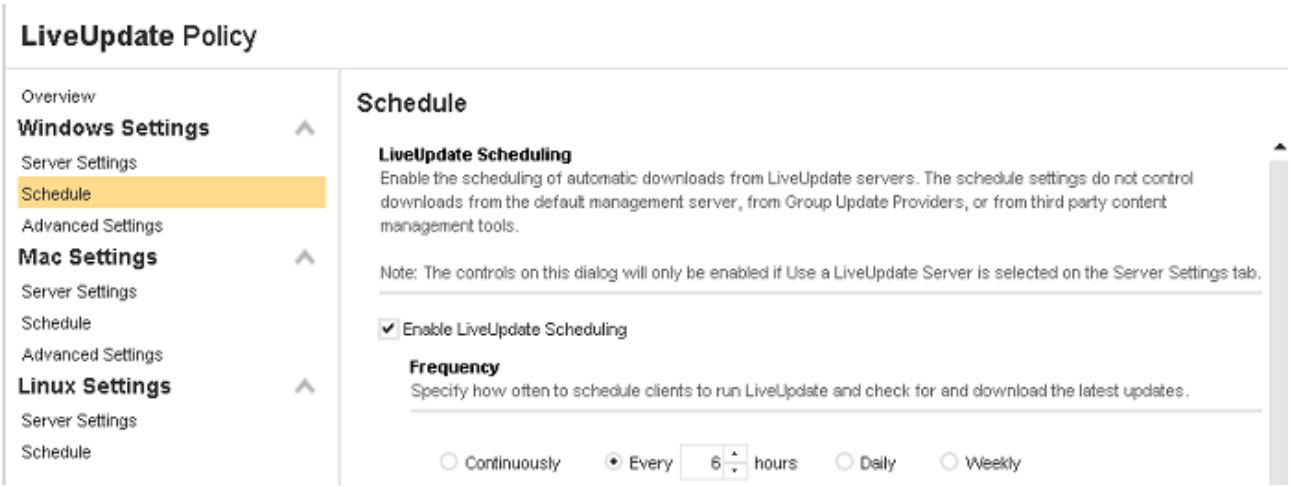


Ilustración 15: Programación de actualizaciones

9. Toma de especificaciones

Se debe realiza una toma de especificaciones previa, respecto al comportamiento esperado del sistema antivirus, el cual sirva de base sobre el cumplimiento de políticas y medidas de seguridad a implantar en la Organización.

Estas medidas pueden marcan no solo el comportamiento de los equipos de la Organización, también establecen las reglas que puedan afectar a equipos de terceras compañías que deban estar conectadas a la Red interna, es por ello importante tenerlas especificadas y documentadas para que puedan estar accesibles para su consulta.

Definimos 3 niveles de políticas:

- Nivel Reducida: Política con protección reducida para equipos que por su desempeño, el antivirus puede provocar problemas de rendimiento. Normalmente aplicara a equipos obsoletos o con pocos recursos, pero también puede aplicar a equipos con un uso intensivo de aplicaciones criticas para la Organización. La aplicación de dicha política se realiza a demanda tras detectar una incidencia en ellos.
- Nivel Estándar: Política por defecto para todos los equipos de la organización.
- Nivel Avanzado: Política con protección avanzada para equipos con necesidad de seguridad extra, por ejemplo equipos conectados a redes publicas o usados por

profesionales que requieren un nivel de seguridad mas avanzado en sus equipos. La aplicación de dicha política se realizara a demanda mediante solicitud cuando se detecte dicha circunstancia.

Los requisitos óptimos para SEPM comienzan en procesadores Pentium IV (procesador mínimo PIII) con 1 GB de RAM (512 MB mínimo). Aún con estos requisitos, el disponer de una política reducida proporciona una solución en caso de que en algunos equipos se pueda producir un riesgo en su rendimiento debido a la instalación del antivirus.

La toma de especificaciones se incluyen en el Anexo I de dicho documento.

10. Definición de políticas de configuración

La definición de políticas del antivirus permite que distintos equipos, por su ubicación, finalidad, características, etc, puedan disponer de una configuración acorde a su desempeño, funcionalidad o capacidad.

Las políticas pueden estar diseñadas para un uso presente o futuro, hasta que no son aplicadas a un grupo de equipos no son usadas. Estos grupos se definen en las ubicaciones, la cual trata de reflejar el diseño propuesto para el entorno de aplicación, factores que afectan a este diseño son las propias ubicaciones físicas o los tipos de dispositivos que podemos encontrar en ellas.

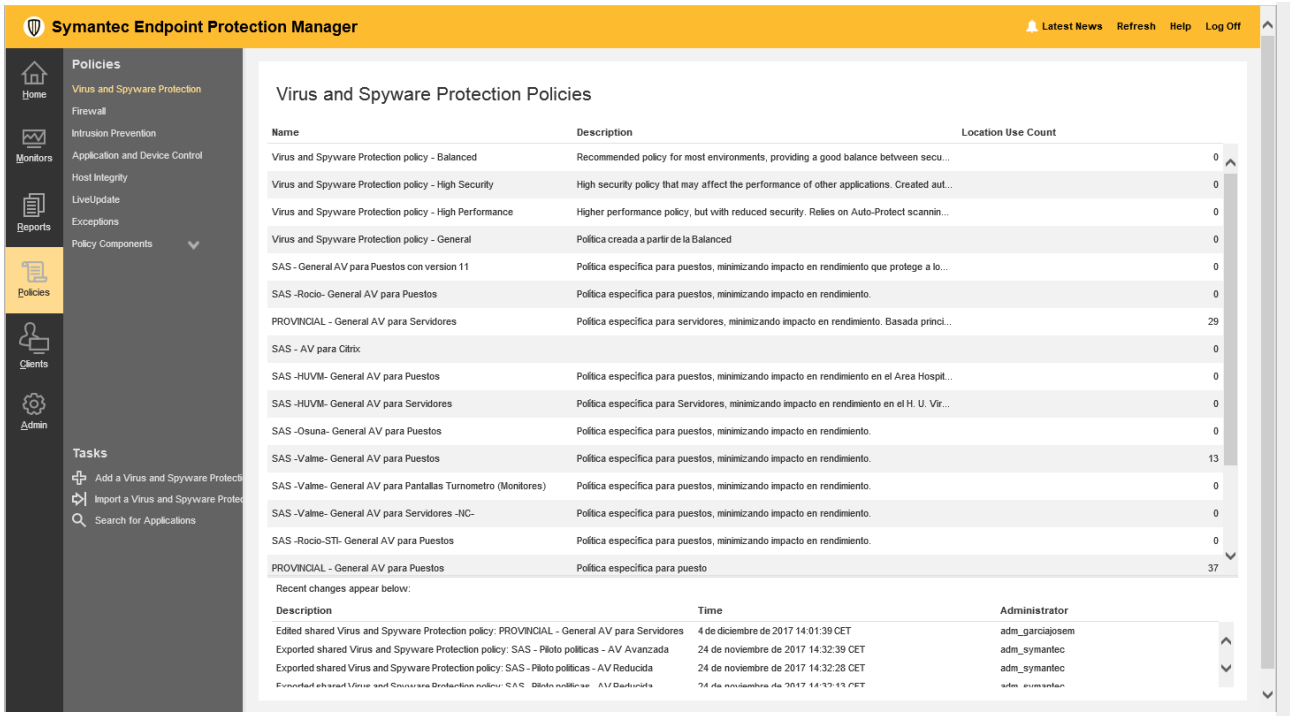


Ilustración 16: Políticas de protección frente a Virus y Spyware

Las políticas permiten propiedades como herencia, por lo cual, dado que la definición de la estructura de la compañía tiene forma de árbol, es posible definir una política general para todos los equipos, aplicarla a la raíz (llamada inicialmente “My Company”), desactivando herencia y aplicado una nueva política en aquellas ramas que así lo requieran:

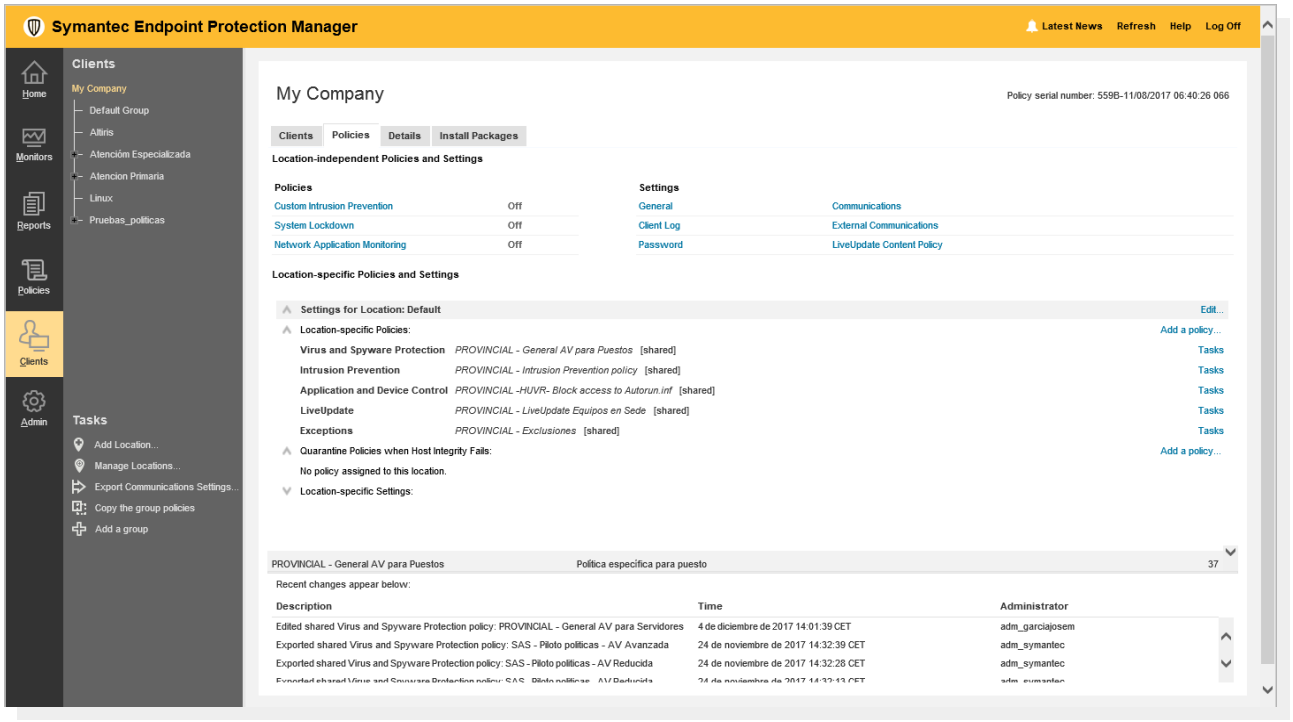


Ilustración 17: Estructura y politicas aplicadas nivel general

Para generar una nueva configuración de la política se realiza las siguientes acciones:

- Hacer clic en Políticas > Protección antivirus y antispyware.

  Las políticas existentes aparecen en el panel derecho.

  Cree una nueva política o copie una política existente
- Se genera en Tareas, en Agregar una política de protección antivirus y antispyware.

También es posible copia y modificar una política existente:

- Con el botón derecho en la política que desea copiar y, a continuación Copiar.
- En el panel derecho, botón derecho y, luego, Pegar.
- Modificar con las nuevas restricciones.

En la tabla 1: políticas de seguridad Endpoint, se han establecido una serie de requisitos para establecer las políticas, que rigen a todos los equipos de la organización, es por ello que la estructura de equipos por centros no debe regir la implementación de ellas y serán configurados de forma uniforme a lo largo de todas las sedes.

Los equipos de Symantec Technology and Response (STAR) y Symantec Endpoint Protection (SEP) desarrollaron una postura de seguridad recomendada para Endpoint Protection, es por ello que el producto incorpora 3 políticas iniciales llamadas: Balanced, High Security y High Performance (Symantec, Configuración de seguridad recomendada para Endpoint Protection)

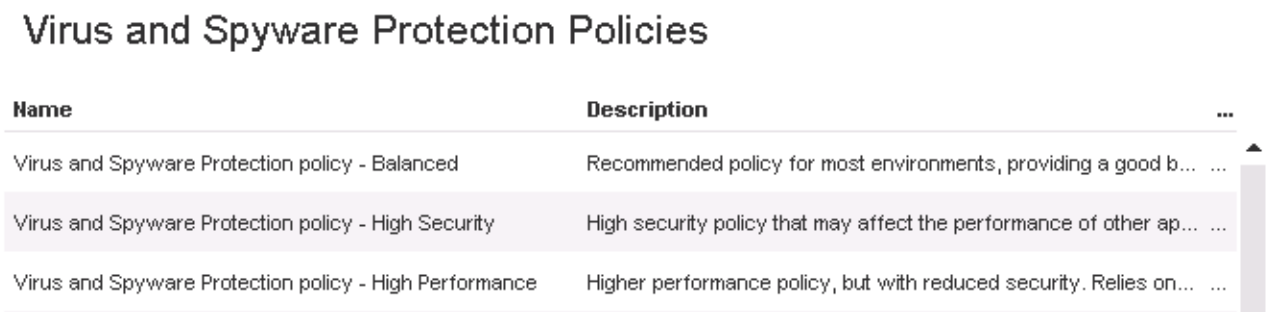


Ilustración 18: Políticas por defecto SEPM

Estas tres políticas se corresponden con el diseño propuesto por la Organización, es por ello que se utilizaran de referencia, serán clonadas y modificadas en las opciones especificas descritas por la Organización en el apartado “Toma de especificaciones”.

Se describen la implementación de estas políticas en los siguientes apartados.

10.1. Políticas de protección frente a Virus y Spyware

Tal como es indicado por Symantec (Guía Administración, p.350) , se referencía que la Política de protección antivirus y antispyware proporciona la protección siguiente:

- Detecta, elimina y repara los efectos secundarios del virus y los riesgos para la seguridad mediante firmas.

- Detecta las amenazas en los archivos que los usuarios intentan descargar usando los datos de reputación de Diagnóstico Insight de descargas.
- Detecte las aplicaciones que muestran comportamiento sospechoso usando heurística y datos de reputación de SONAR.

Para estas funciones, se dispone de dos características adicionales:

- Auto-Protect: Es la primera linea de defensa del antivirus, analiza en tiempo real las amenazas en los archivos manejados por el equipo en tiempo real. Cualquier acción sobre un fichero: acceso, copia, guardado, apertura y cierre, provoca la monitorización dicho fichero.
- Basada en reputación: Symantec recolecta información sobre amenazas y facilita esta información de forma que es posible conocer posibles casos de amenazas en casos como descarga de ficheros de internet. De esta forma es posible establecer criterios como no ejecución de ficheros con mala reputación (=<level-5), o bien ser mas restrictivos permitiendo solo ficheros con buena reputación (=>level-6). Una alta sensibilidad en este sentido puede provocar un alto riesgo de detección de falsos positivos.

a) Programación de escaneos

Se parametriza, en función del tipo de política, las programaciones:

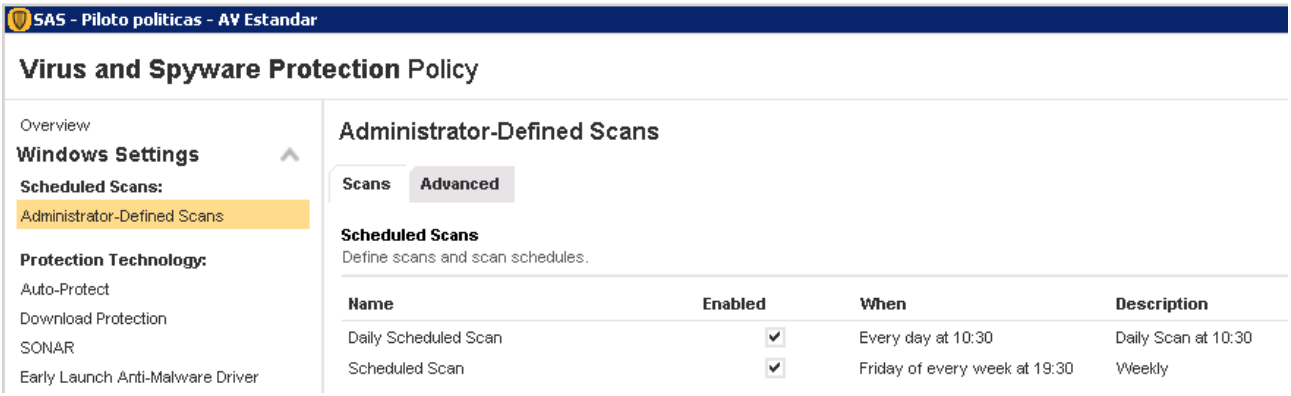


Ilustración 19: Configuración programación escaneos política estándar

La revisión debe tratar de ajustarse a los horarios en los que la mayoría de los equipos permanezcan encendidos y en momentos de menor uso, ese intervalo ha sido aplicado en esta implementación en el momento del descaso de la mañana.

Y los tipos:

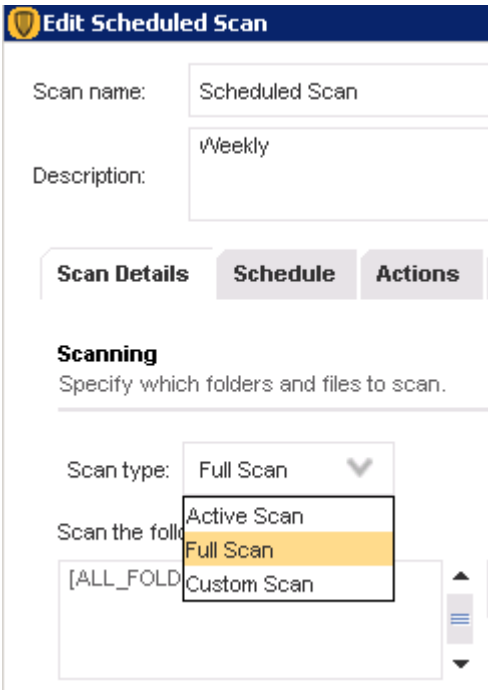


Ilustración 20: Tipos de escaneos

Opciones de profundidad en ficheros compartidos:

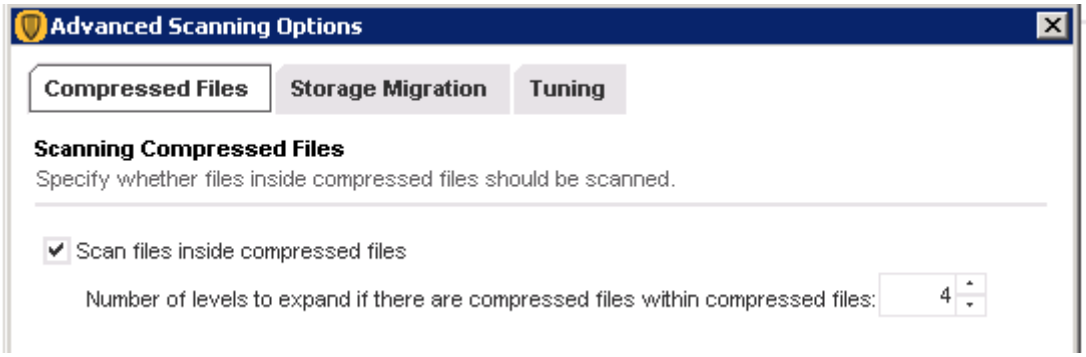


Ilustración 21: Profundidad ficheros comprimidos

Configuración de rendimiento:

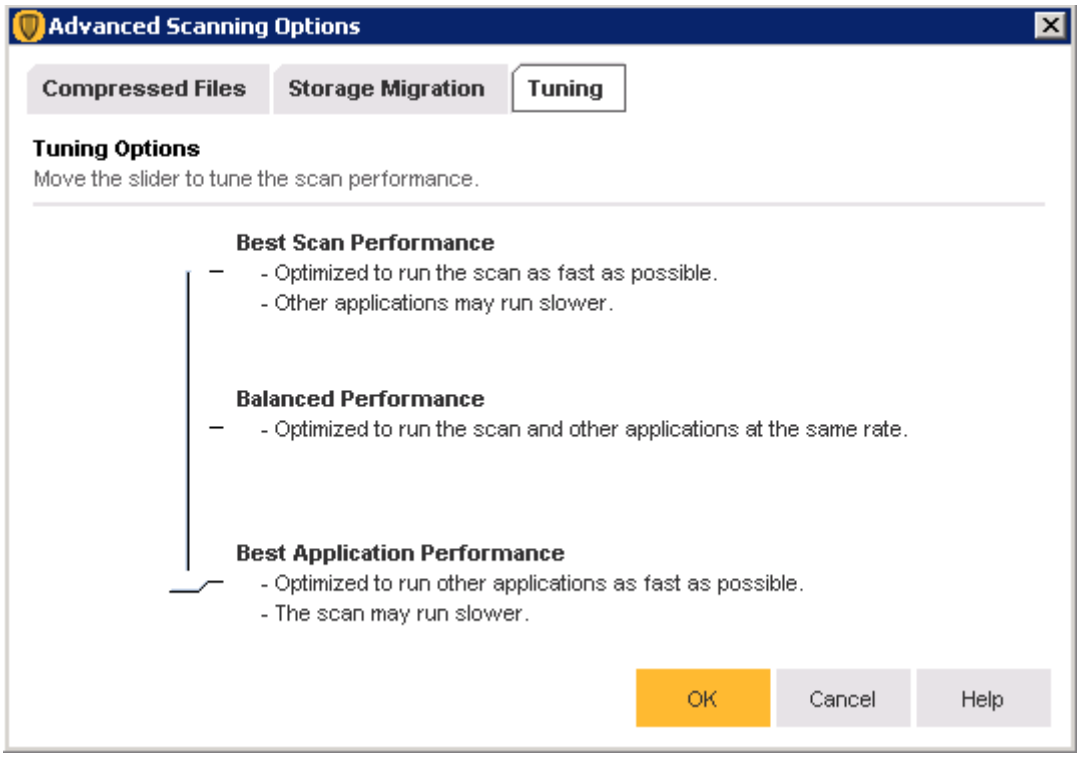


Ilustración 22: Rendimiento durante escaneo

Acciones a realizar ante detecciones:

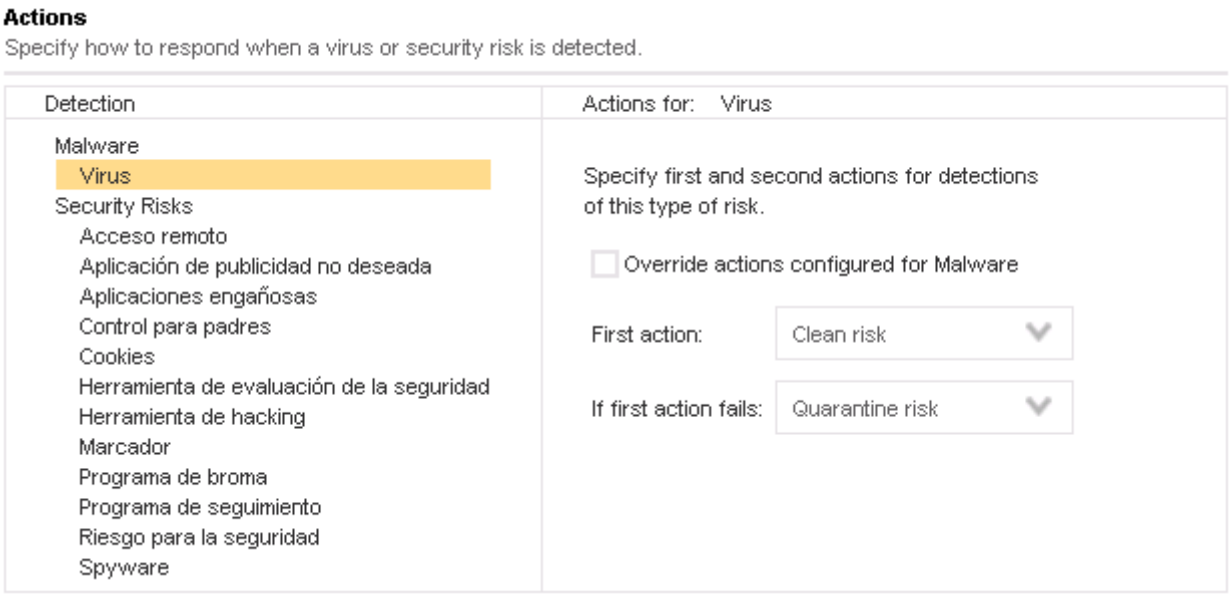


Ilustración 23: Acciones a realizar antes riesgos detectados

Los riesgos para la seguridad son programas que no son intencionalmente maliciosos, pero pueden suponer un riesgo para la seguridad si son instalados en el sistema, por ejemplo usados como caballos de Trolla para la posterior infección.

b) Análisis en tiempo real

Se provee la configuración para el sistema proactivo que analiza en tiempo real el sistema en busca de elementos que pueden provocar amenazas.

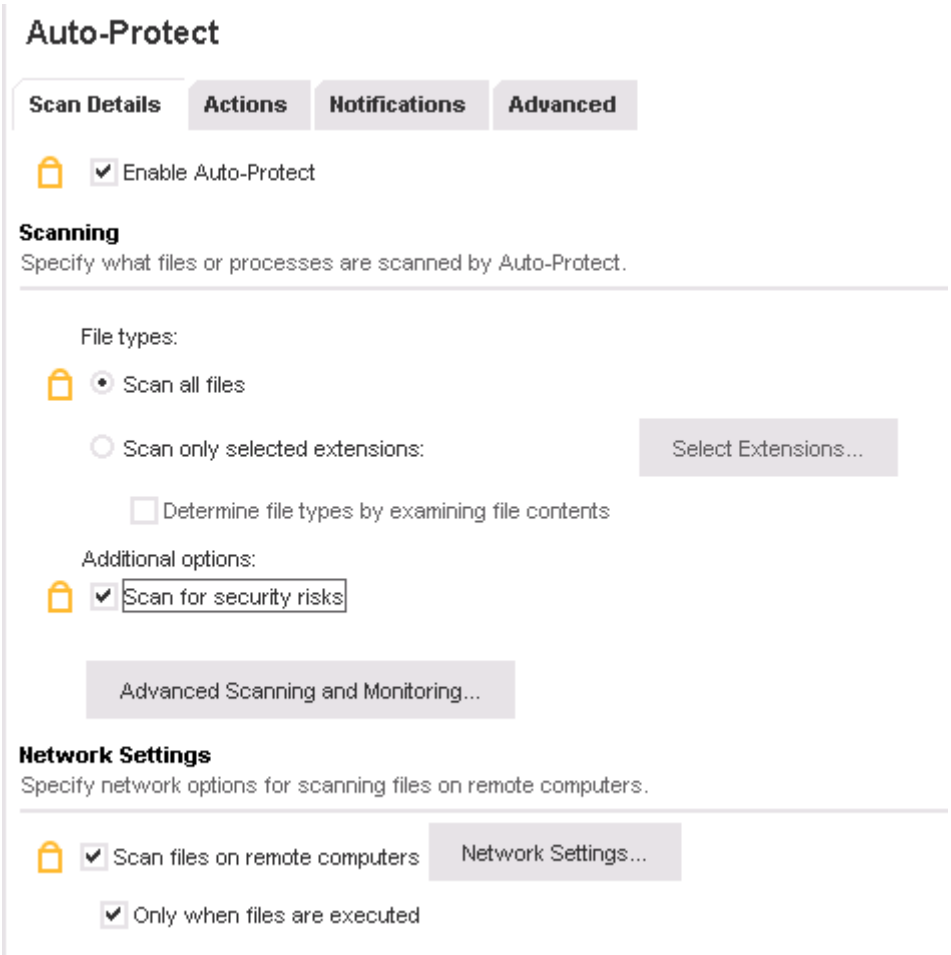


Ilustración 24: Sistema de auto-protect

Es posible implementar opciones avanzadas, como el seguimiento de riesgos que permite resolver la información del equipo remoto que provoca la infección o la configuración avanzada de riegos que permite revisar bien sectores de arranque durante la conexión de

dispositivos re-movibles o el fichero durante su acceso o modificación, a la vez que ficheros en unidades de red conectadas.

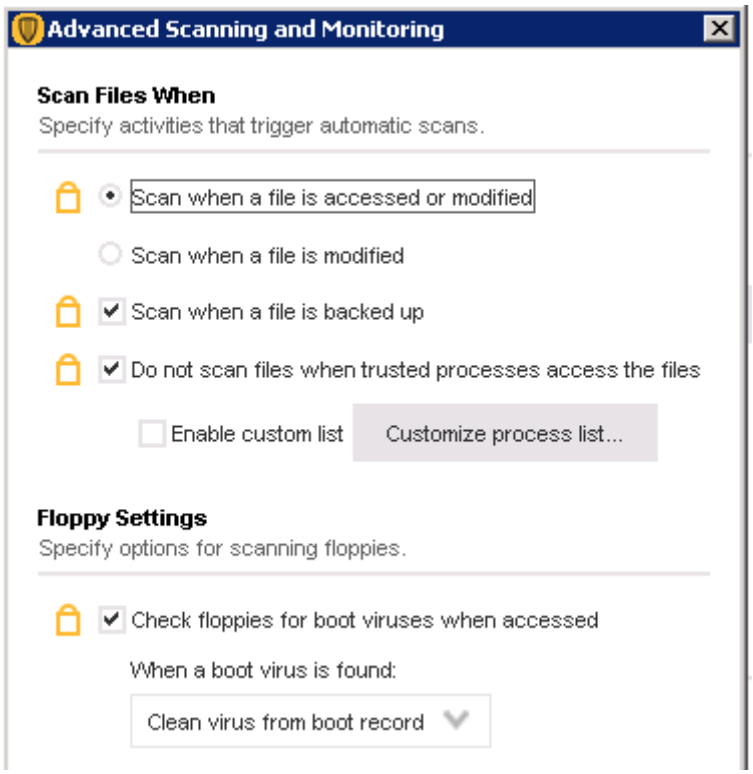


Ilustración 25: Opciones avanzadas de escaneo y monitorización

c) Configuración de reputación

Se debe configurar la activación de la reputación, para versiones de SEPM 12.x se activara en la configuración del escaneo:

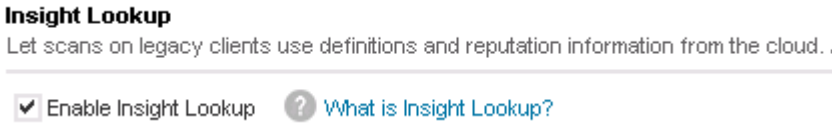


Ilustración 26: Insight para clientes 12.x

Es importante también definir el origen de la información de reputación.

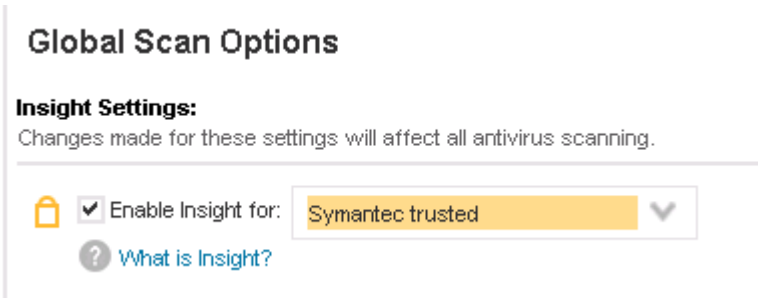


Ilustración 27: Configuración origen de reputación

Se configura el nivel de sensibilidad:

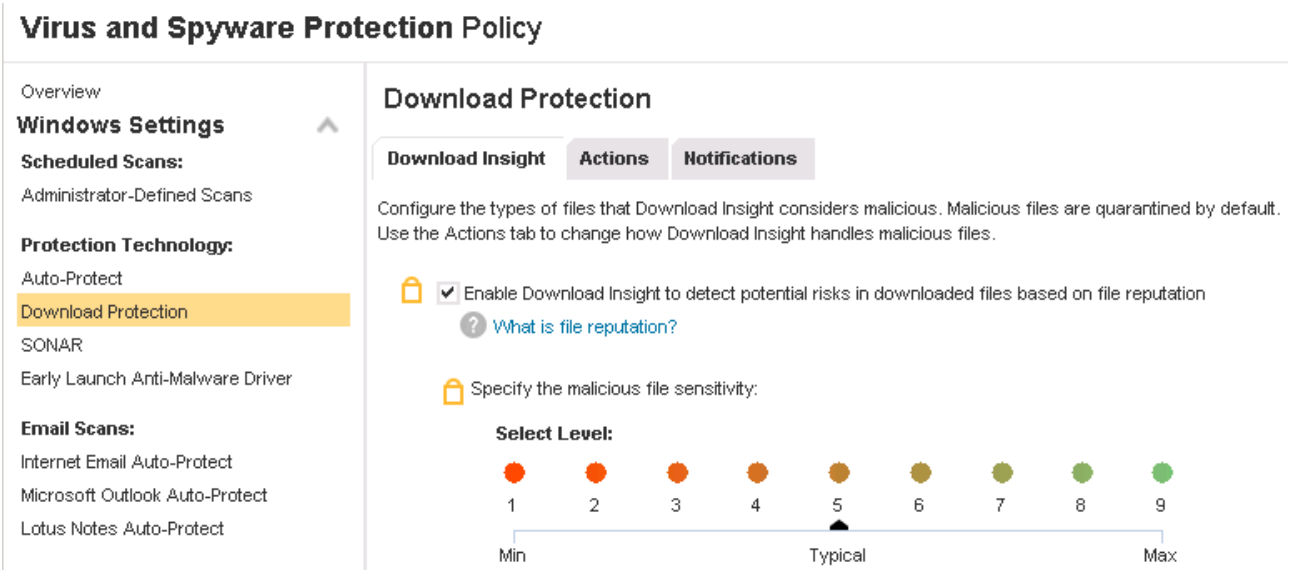


Ilustración 28: Sensibilidad reputación

d) Configuración Heurística

La protección heuristica, ademas de los datos de reputación, ayudan a detectar nuevas amenazas que aun no son controladas por las firmas antivirus. Estas amenazas, también llamadas día cero, se controlan con el modulo llamado SONAR.

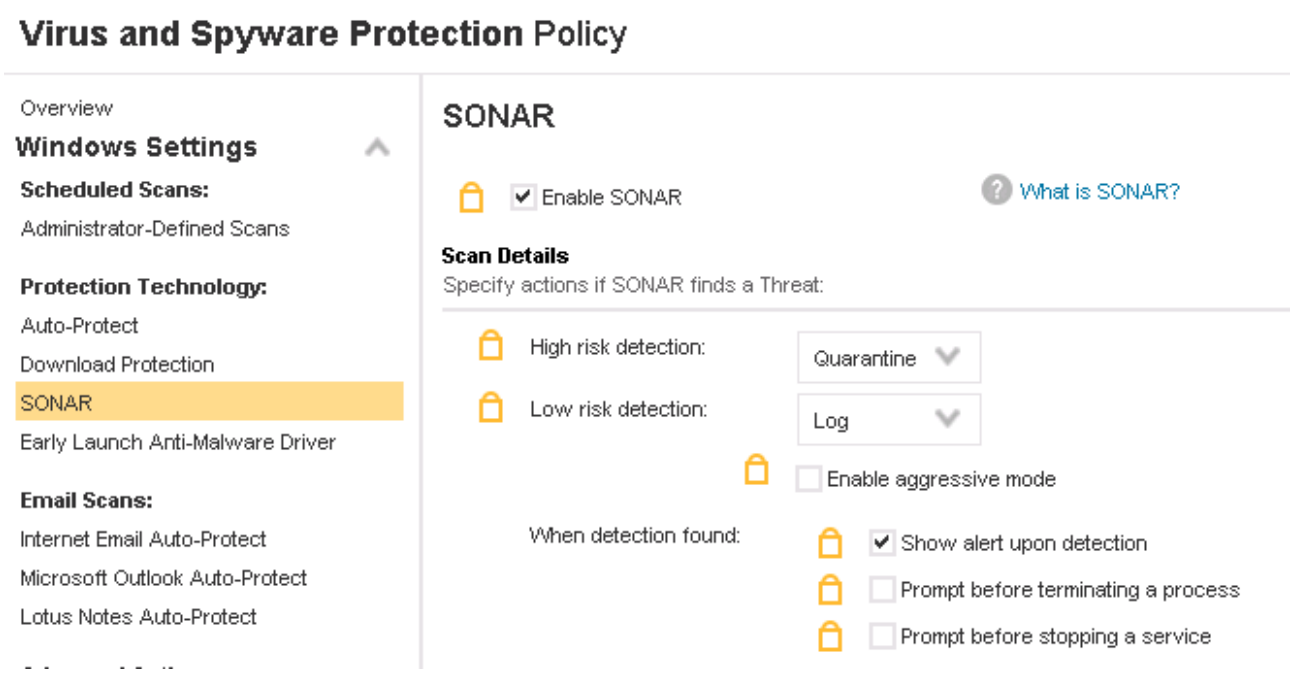


Ilustración 29: Activación de SONAR

Las operaciones detectadas como provocadas por software mal intencionado pueden incluir, además del comportamiento sospechoso, cambios en la configuración de red.

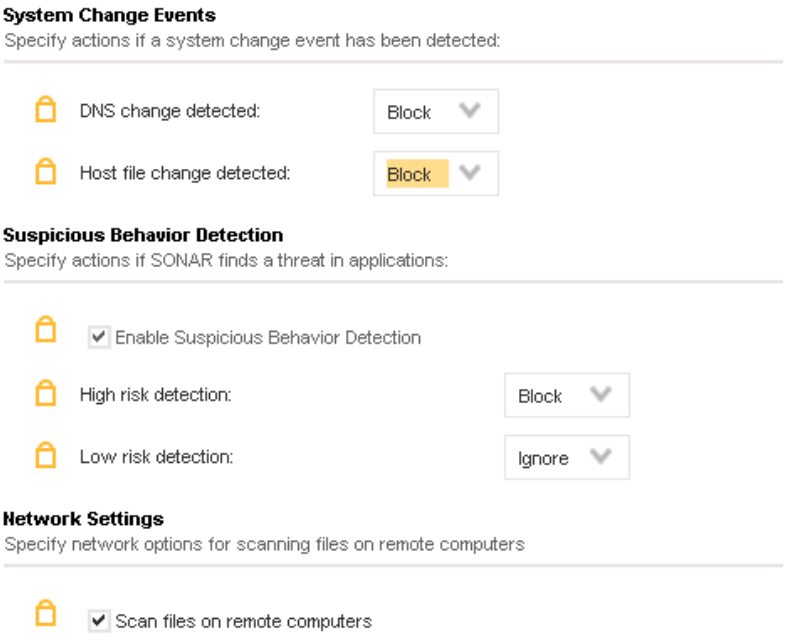


Ilustración 30: Comportamiento SONAR

e) Protección del correo

El correo electrónico es una de las herramientas mas utilizadas para la comunicación por la Organización, a la vez es uno de los medios mas utilizados para la distribución de malware.

Se debe activar dicha protección y personalizar las opciones especificas para realizar la protección antivirus acorde con la funcionalidad definida.

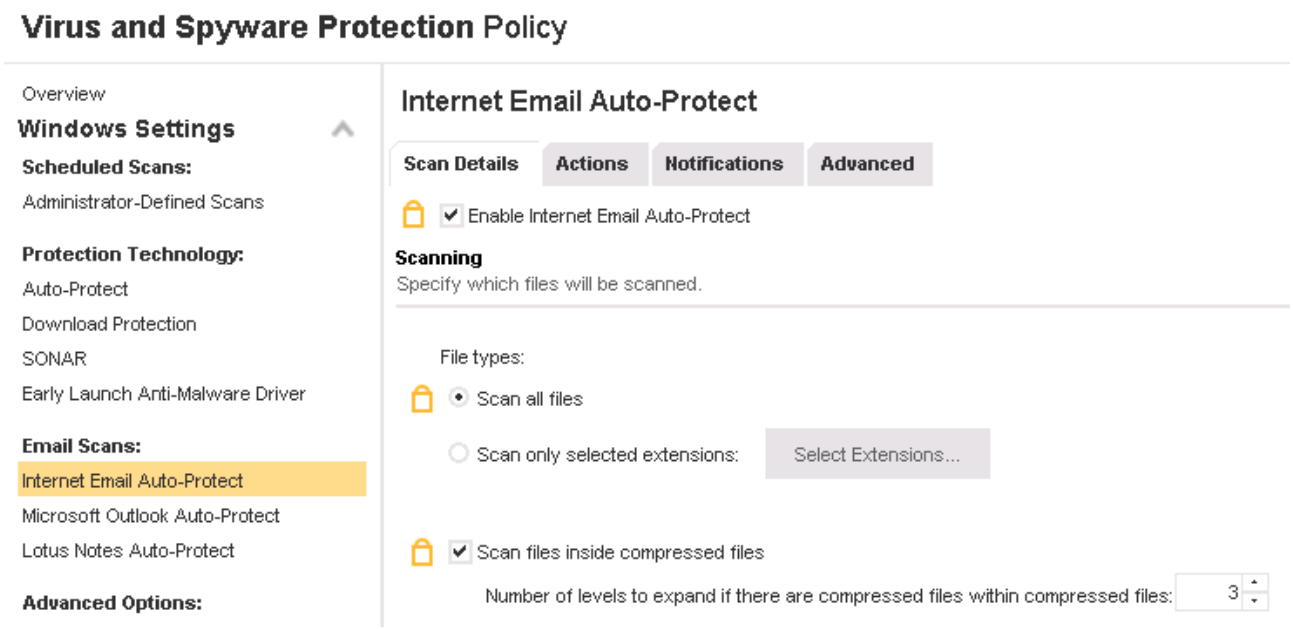


Ilustración 31: Protección correo electrónico

f) Cuarentena

Una de las opciones mas utilizadas, una vez detectado un riesgo, es su inclusión en un sistema de cuarentena el cual permite, tanto aislar el fichero del resto de la información, a la vez que tratar de realizar acciones como la restauración del fichero a un estado optimo, por ejemplo tras la inclusión de un fichero de firmas que permita esta acción sobre el riesgo detectado.

En caso de que no se puedan realizar estas acciones tras un tiempo delimitado, es preciso eliminarlo del sistema cliente. Los ficheros de este tipo solo deben conservarse en equipos destinados específicamente para investigación de estos incidentes.

Configuración de la cuarentena:

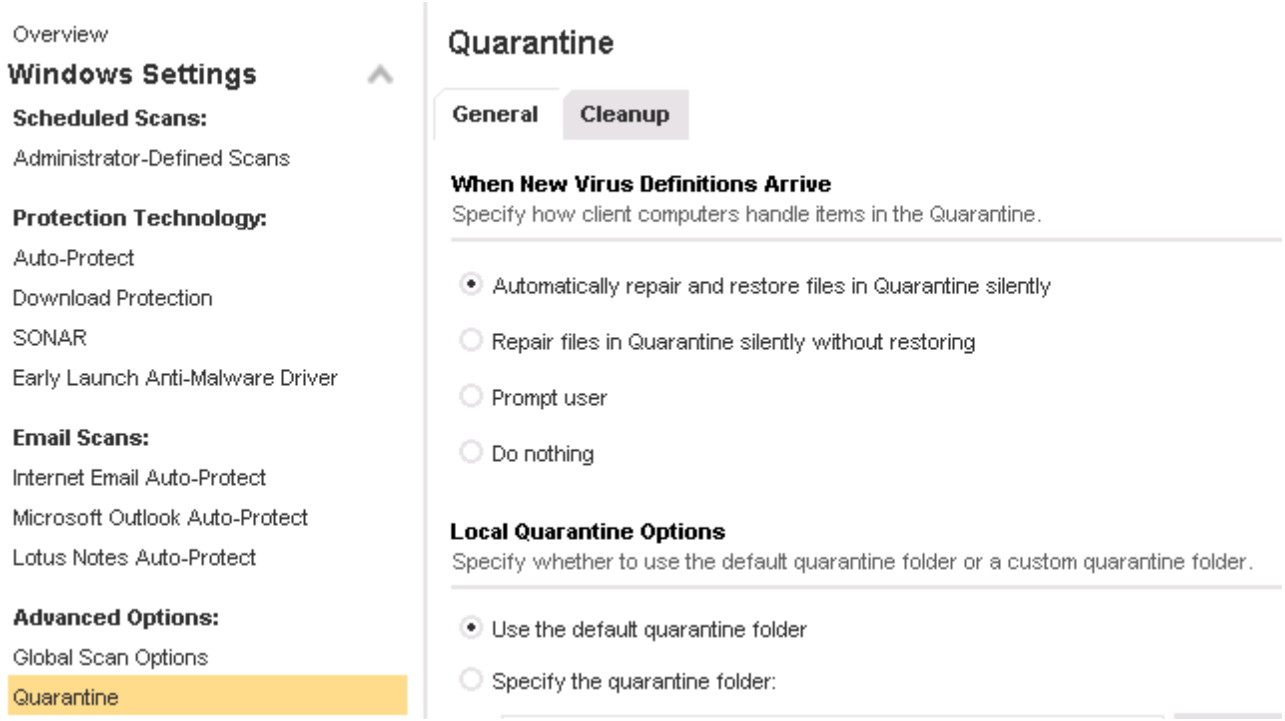


Ilustración 32: Configuración de cuarentena

10.2. Políticas de actualización

La configuración de estos parámetros permite la configuración de las actualizaciones de firma antivirus para los clientes SEP. Esta configuración se debe adaptar a la arquitectura definida en la Organización, capitulo “Arquitectura de la plataforma”, donde se indicaba el uso de un servidor de LiveUpdate y de determinados GUP por sedes, para de esta forma controlar el riesgo que puede producir en los recursos del servidor SEPM la petición de actualizaciones por parte de todos los clientes SEP.

La política que configura las actualizaciones de los clientes, se apoyara en la correcta configuración del servidor, respecto al servidor de actualizaciones generales (LiveUpdate):

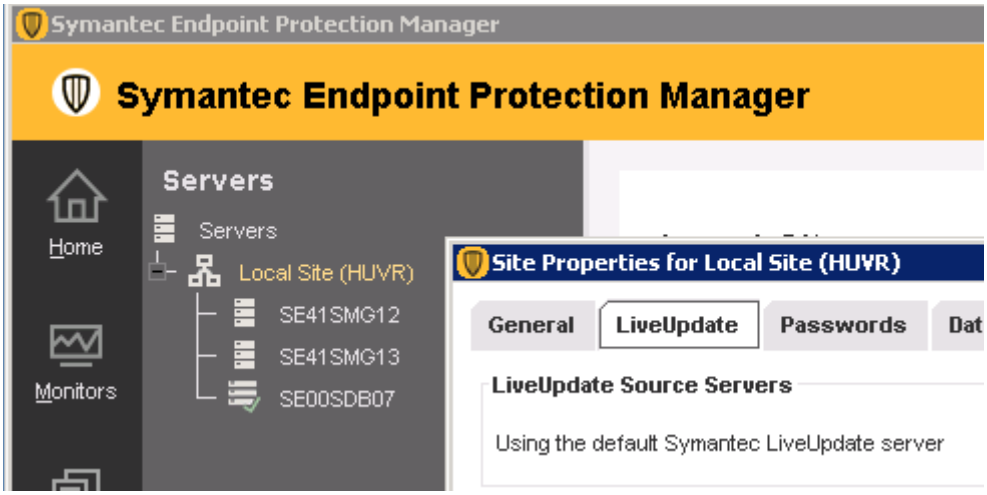


Ilustración 33: Configuracion actualizaciones SEPM

Para la configuración de las actualizaciones en los clientes (SEP), se debe configurar la política de LiveUpdate, donde a nivel general indicaremos que utilice el servidor por defecto de LiveUpdate junto con el servidor SEPM:

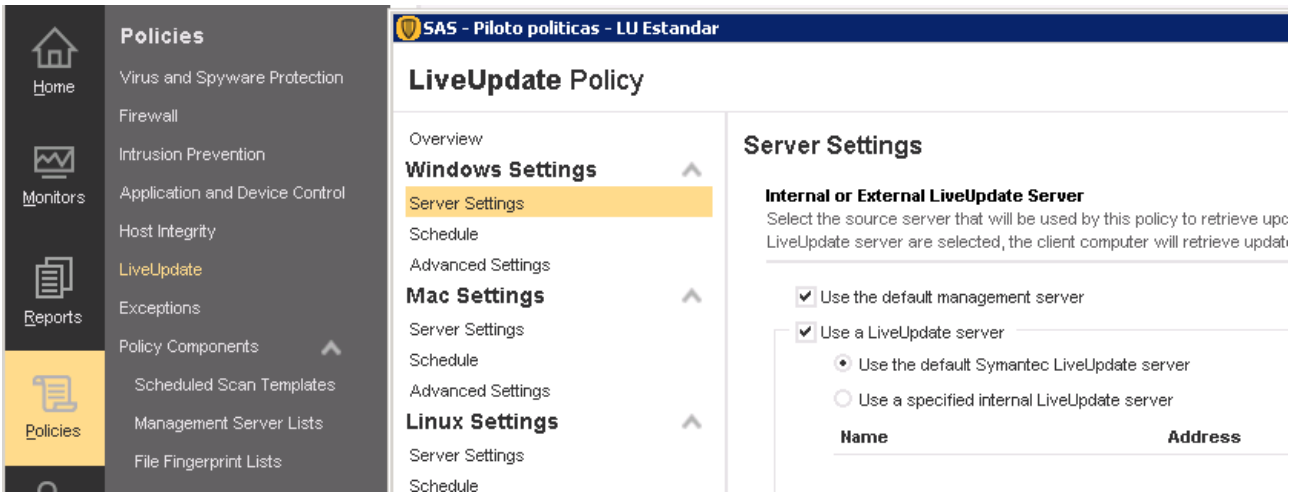


Ilustración 34: Configuración política general LiveUpdate

A continuación se describe la configuración para el uso de un servidor GUP para la distribución de firmas de antivirus, dado que por la definición de la arquitectura del proyecto es obligatorio para las sedes con un ancho de banda limitado, y recomendable en el resto de sedes.

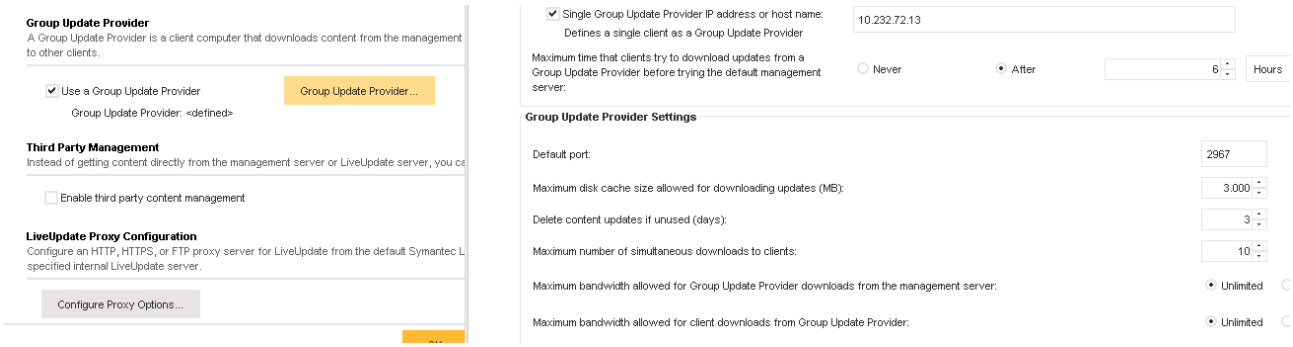


Ilustración 35: Configuración GUP en Sedes

Desde esta opción se indicara la dirección IP del equipo asignado para realizar las tareas de distribución de firmas en la sede correspondiente, a la vez que podemos establecer otra serie de valores como el puerto TCP usado para comunicar con los clientes.

Finalmente queda configurada la frecuencia de consultas de actualizaciones en la programación de la política:

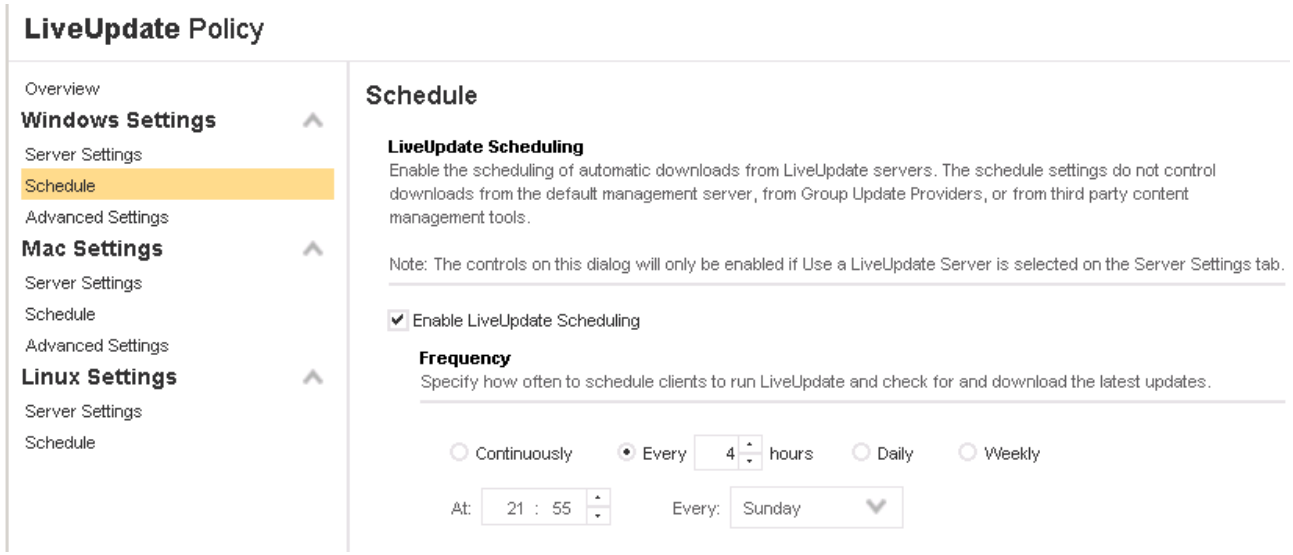


Ilustración 36: Frecuencia de actualizaciones

La frecuencia de consultas de actualizaciones debe ser menor a la frecuencia en la cual tanto el servidor es actualizado, cada 6 horas, como el periodo de tiempo que el proveedor (Symantec) libera las nuevas versiones, 3 veces al día. De esta forma lo periodos en los cuales los clientes podrán encontrarse en una ventana de tiempo con firmas desactualizadas sera menor, por contra podemos incrementar el ancho de banda usado en la red durante las consultas al servicio de actualizaciones.

10.3. Protección contra amenazas de red

Existen una serie de políticas de antivirus para evitar los ataques externos sobre los clientes.

Dentro de estas políticas que aplican a este perfil, se encuentran:

- Política de firewall

  El objetivo es permitir o bloquear la comunicación por red entre distintos equipos o servicios mediante la configuración de reglas de firewall. Estas reglas deben ser complementarias a las existentes en los firewall de seguridad perimetral instalados en las Sedes de la Organización.

- Política de Intrusion Prevention

  La prevención de intrusiones debe detectar y mitigar los ataques se puedan producir en la red. Estos ataques pueden provenir desde aplicaciones con conexión a otras redes, como son los navegadores web, aplicaciones java, etc. Es un servicio complementario al firewall, y analiza cada paquete de red buscando modelos que se corresponde con ataques. Estos modelos también pueden ser diseñados por los administradores del sistema antivirus.

El orden de procesamiento de la protección de red es el siguiente:

Prioridad	Configuración
Primer lugar	Firmas IPS personalizadas
Segundo lugar	Configuración de la prevención de intrusiones, configuración del tráfico y configuración de ocultación
Tercer lugar	Reglas integradas
Cuarto lugar	Normas de firewall
Quinto lugar	Comprobaciones de análisis de puertos
Sexto lugar	Firmas IPS que se descargan con LiveUpdate

Tabla 10: Prioridad de protección de red

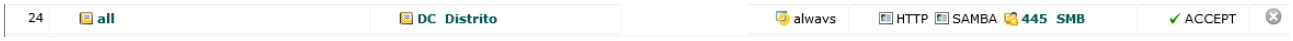
a) Política firewall

Dado que la Organización dispone de firewall perimetrales en todas sus sedes, es necesario adaptar esta política a esta situación, así se establece el siguiente orden del filtrado:

- Filtrado en firewall perimetrales del trafico no permitido.
- Filtrado en firewall antivirus del trafico o servicios permitidos.
- Resto del trafico debe ser denegado en Firewall antivirus.

Se indica una regla especifica, para tomar como referencia en base al las reglas generales establecidas y que deben ser proporcionadas por la Organización. En este caso para la compartición de carpetas entre equipos de la red interna:

- Regla en firewall perimetral Fortigate 50B:



  Permite el trafico SMB hacia los equipos clientes.

- Regla en firewall antivirus que limita a los equipos corporativos la conexión por SMB y corta el retos del trafico:

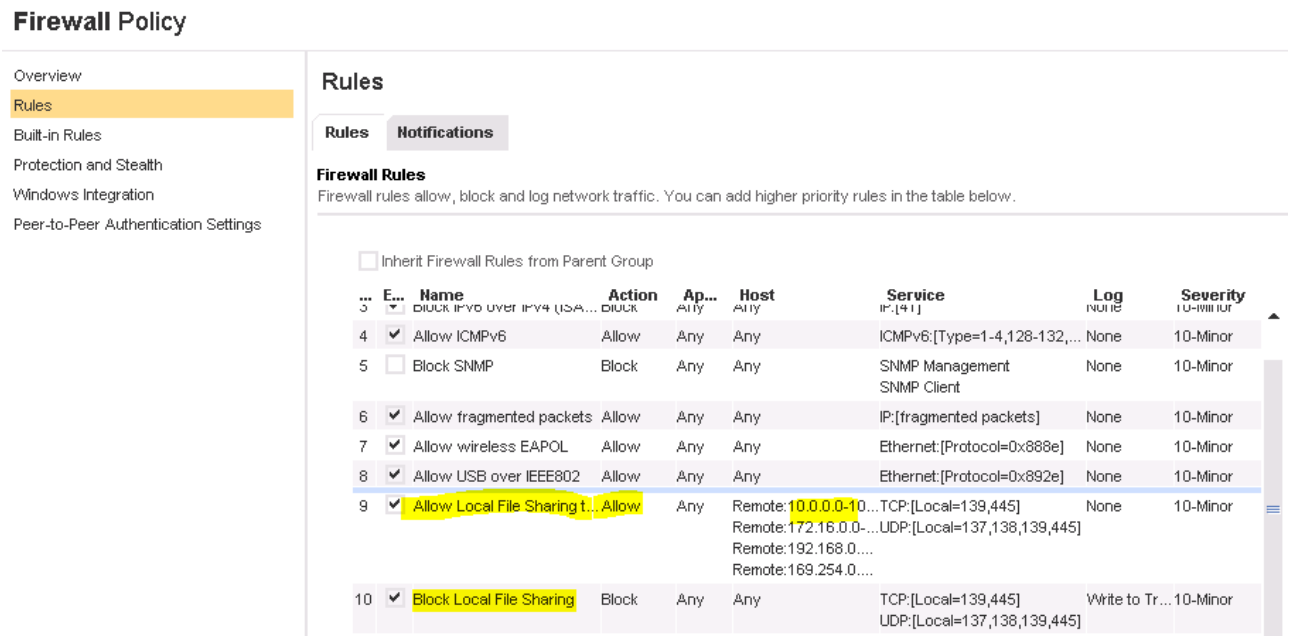


Ilustración 37: Política firewall para SMB

b) Política de prevención de intrusiones

Esta política puede controlar los siguientes tipos de ataques:

- Prevención sobre intrusiones de red.
- Prevención contra intrusiones de navegador.
- Prevención contra vulnerabilidades genéricas.

Inicialmente se debe activar la detección mediante firmas de IPS contra ataques de red o realizados mediante el navegador web, de esta forma el antivirus revisara con los patrones actualizados el trafico de red hacía el host. En caso de detectar algún tipo de ataque, realizara el bloqueo del mismo.

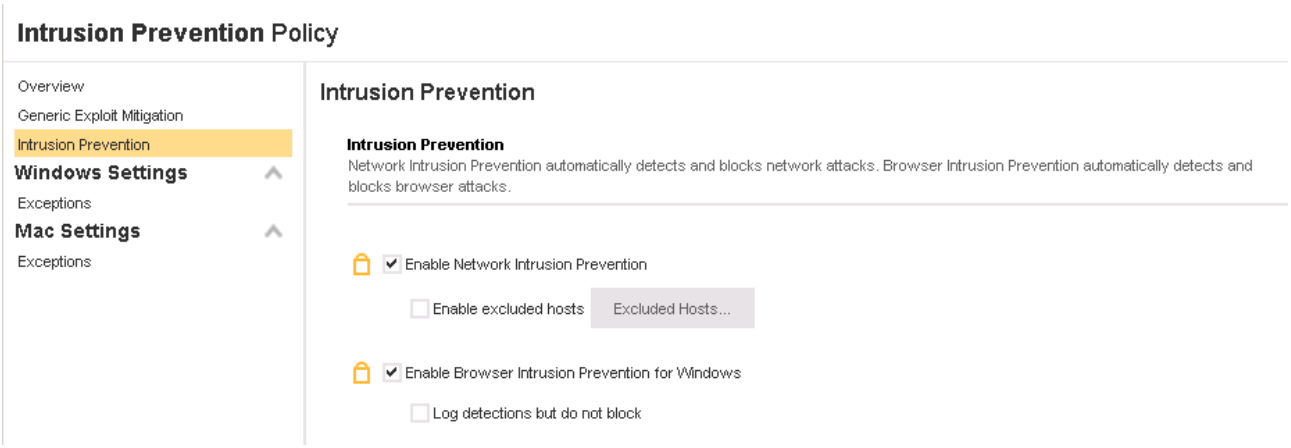


Ilustración 38: Activación IPS

La activación de la mitigación genérica de ataques de vulnerabilidades de aplicaciones, cubren los ataques hacía:

- Prevención en Java

  Bloquea ataques en applets Java que intentan deshabilitar el servicio de “Windows Security Manager” y de esta forma permitir la ejecución de codigo Java con elevación de privilegios.

- Ejecución de código arbitrario

  Protege las vulnerabilidades que permiten, a un atacante, utilizar ubicaciones de memoria para ejecutar código sin autorización.

- Protección sobre la sobreescritura

  Protege cuando controlando que el flujo de ejecución del código no modifique el manejador de la pila de excepciones, provocando un desbordamiento del búfer de la misma.

Sin embargo, aun activada esta opción, se debe realizar una política general de actualización de versiones de las aplicaciones en función de las nuevas revisiones que aporten mejoras en la seguridad de las misma, en la mayoría de las ocasiones tras detectar vulnerabilidades de este tipo.

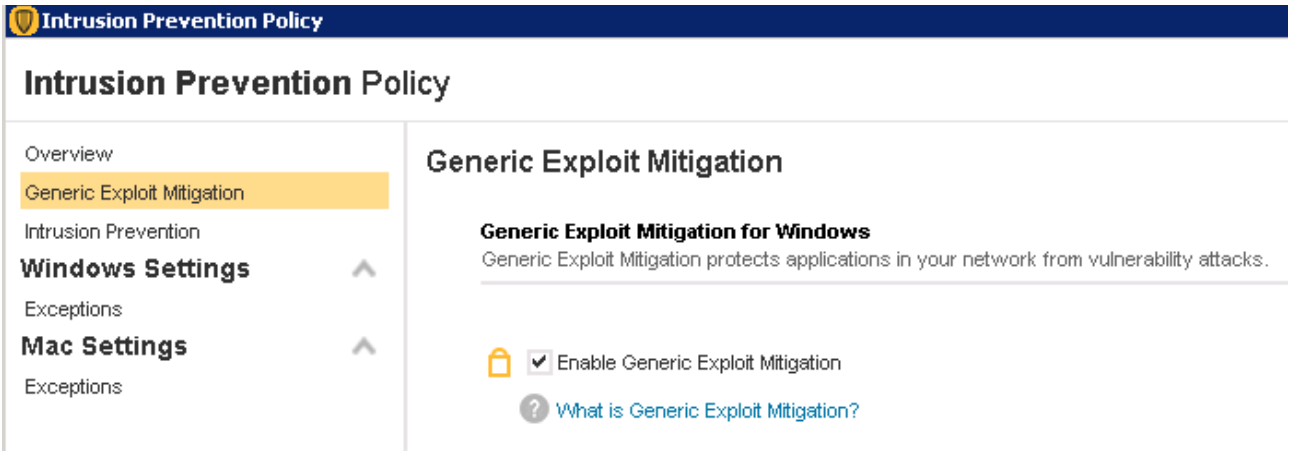


Ilustración 39: Mitigación de ataques genericos IPS

10.4. Control de aplicaciones y dispositivos

Esta política permite supervisar y controlar el comportamiento de las aplicaciones en los clientes SEP y los dispositivos usados en ellos.

Mediante el control y bloqueo de aplicaciones se pueden realizar las siguientes acciones:

- Proteger a las aplicaciones del posible control que un determinado malware pueda realizar en ellas.
- Restringir las aplicaciones que pueden ejecutarse.
- Proteger la configuración frente a cambios producidos por los usuarios no administradores de TI.
- Proteger claves de registro y carpetas criticas del sistema operativo.

Control de dispositivos:

- Permite bloquear diversos tipos de dispositivos, como USB, infrarrojo y dispositivos de FireWire.
- Bloquea puertos de comunicaciones como los puertos serie o paralelos.

Para los dispositivos removibles, se establece en el sistema operativo una búsqueda de un fichero de carga inicial, llamado autorun.inf, que al ejecutarse permite entre otras cosas cargar automáticamente un menú de la aplicación disponible en dicho dispositivo.

Esta característica, es aprovechada por ciertos virus para permitir su ejecución automatizada cuando es introducido un pendrive usb o un CD/DVD en un lector del equipo cliente, por lo cual una medida de protección eficaz es deshabilitar este servicio mediante el antivirus.

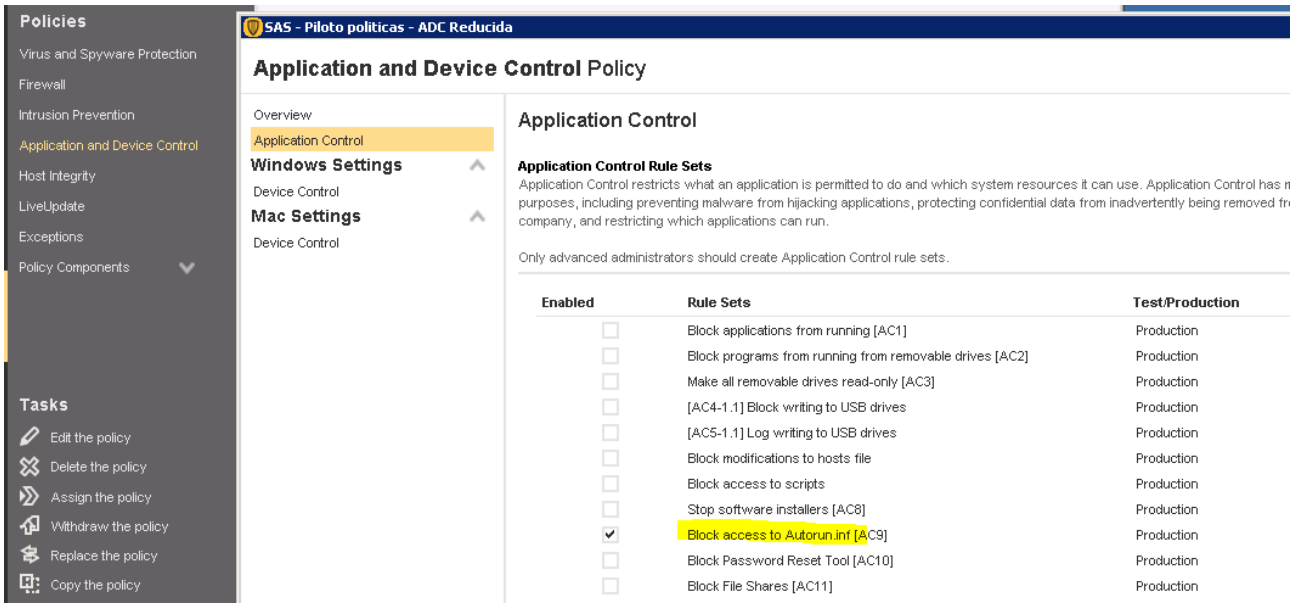


Ilustración 40: Desactivación autorun.inf automáticamente

Para el control de dispositivos, se procede a deshabilitar los puertos usb utilizados como unidades removibles. Un aspecto importante es no anular los HID (Human Interface Device) lo cual requiere un estudio mas complejo, dado que además de ser utilizado por dispositivos como el teclado o ratón, están siendo usado también para realizar ataques dirigidos cuando el hacker tiene acceso físico a los equipos.

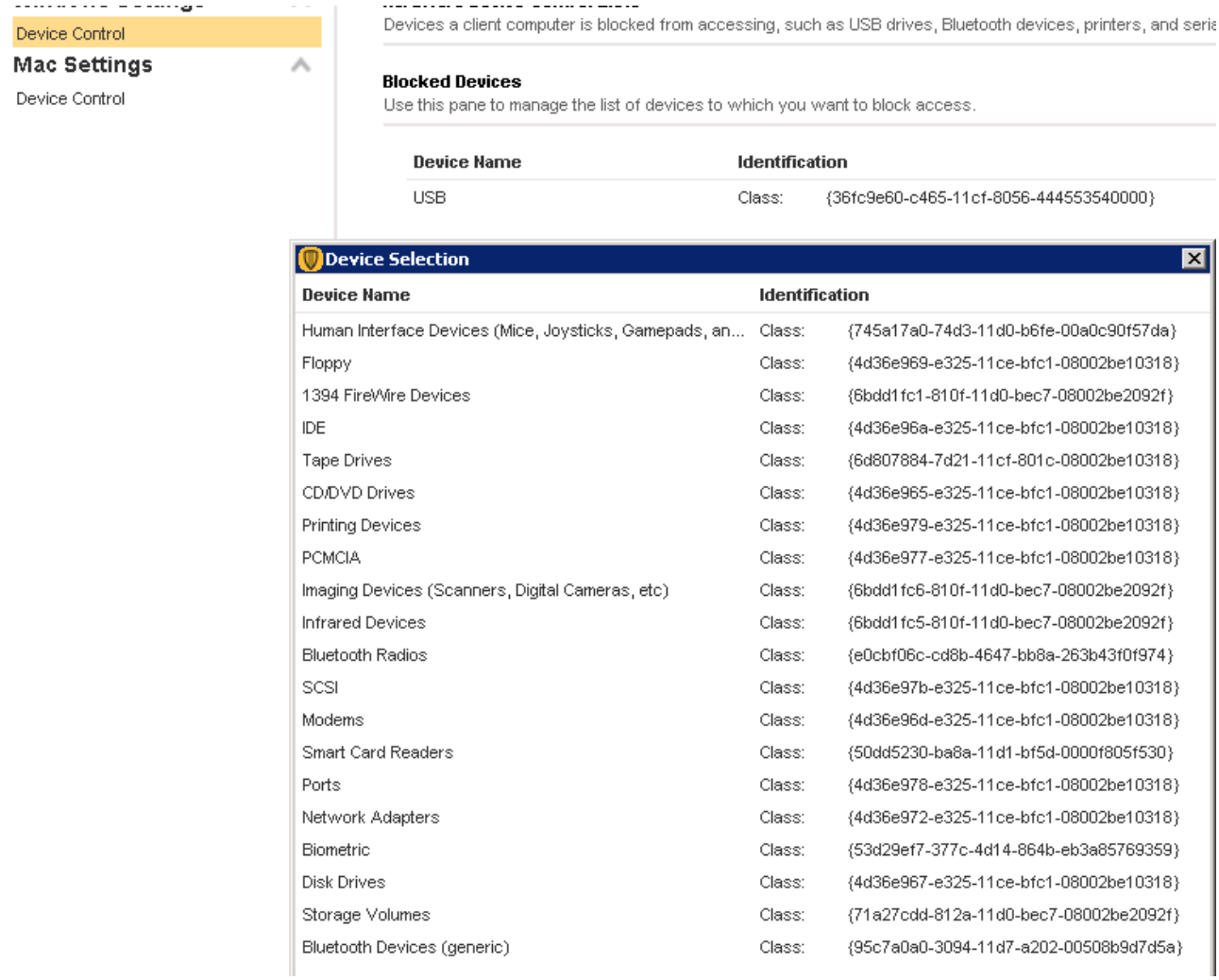


Ilustración 41: Desactivación de puertos USB datos

10.5. Implantación de políticas y pruebas

a) Implantación

La estructura de clientes en esta Organización permite una granularidad en la definición de políticas y configuraciones pudiendo llegar a cada sede. Mediante la definición de estas políticas, se marca un camino general para todas ellas, siendo de aplicación

mandatario las políticas estandar y, aplicadas en casos particulares y autorizados, el resto de políticas.

La aplicación de las políticas se puede realizar de forma general en todas la sedes mediante la configuración de las políticas que aplican a todos sus clientes. Los clientes se encuentran desplegados en el árbol definido en la estructura definida tras la instalación, en la cual se definían todas las sede, a la cual añadimos ahora las ramas para realizar pruebas de concepto y desempeño.

Dentro de cada Rama, en la pestaña de políticas, se debe evitar la herencia y añadir las políticas correspondientes a su definición. Se indica a modo de ejemplo la definición de políticas para la rama: Políticas_estandar

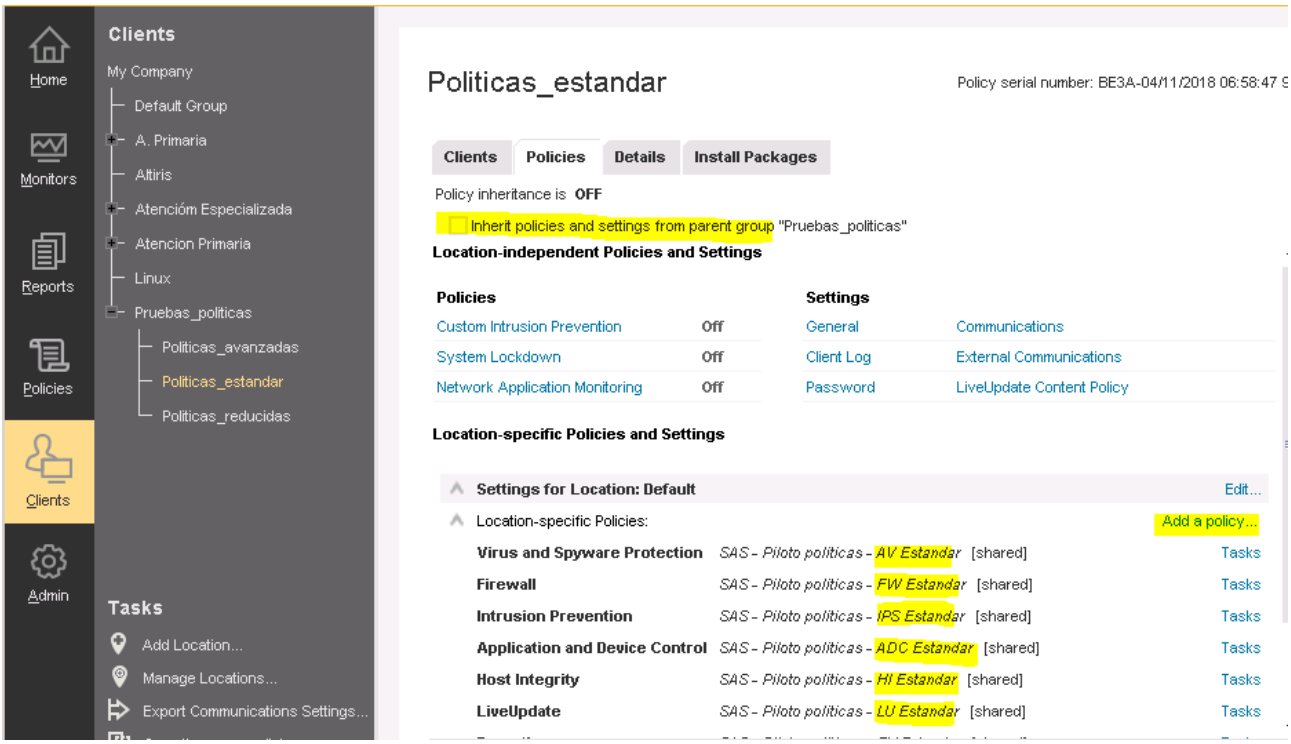


Ilustración 42: Pruebas de políticas

La configuración de las ramas de las sedes se realizara de la misma manera una vez testeadas las mismas.

b) Pruebas

Para comprobar el funcionamiento de los distintos servicios del antivirus, se procede a ejecutar en un cliente SEP las siguientes simulaciones junto con su resultado.

- Protección antivirus y antispyware

  Para probar la protección antivirus y antispyware, se descarga el virus de prueba EICAR desde: http://www.eicar.org/86-0-Intended-use.html

  Donde podemos descargar un ejecutable llamado eicar.com que contiene una secuencia controlada en las firmas del motor antivirus y anti-malware

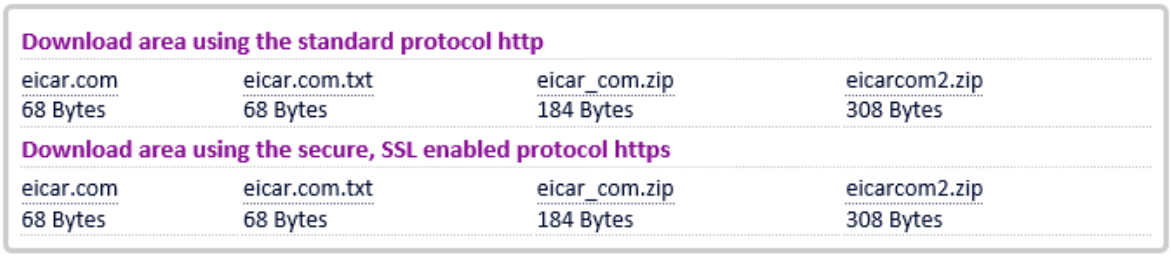


Ilustración 43: Eicar virus test

Tras su ejecución comprobamos la detección del sistema antivirus frente al mismo, revisando por ejemplo el log del sistema local:

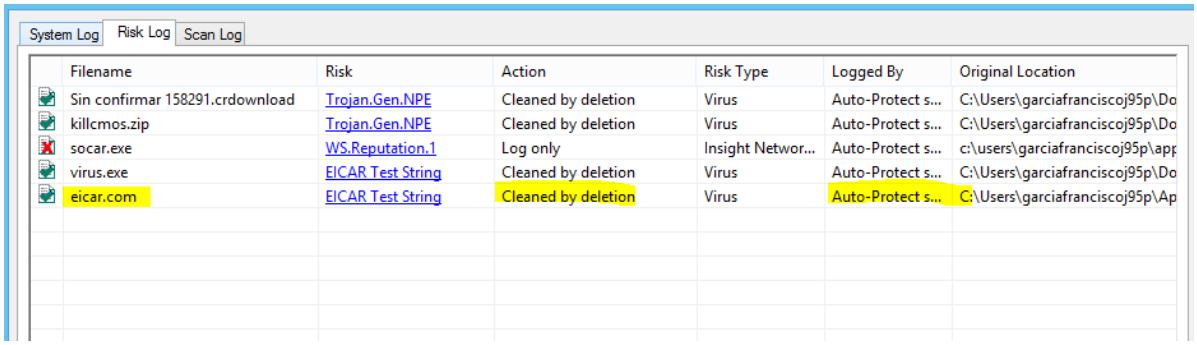


Ilustración 44: Test protección antivirus

- Detección heuristica

  Para testear el motor de protección contra comportamiento, se descarga la aplicación socar.exe desde la web: https://support.symantec.com/en_US/article.TECH216647.html que forzara la actuación de la configuración del modulo SONAR:

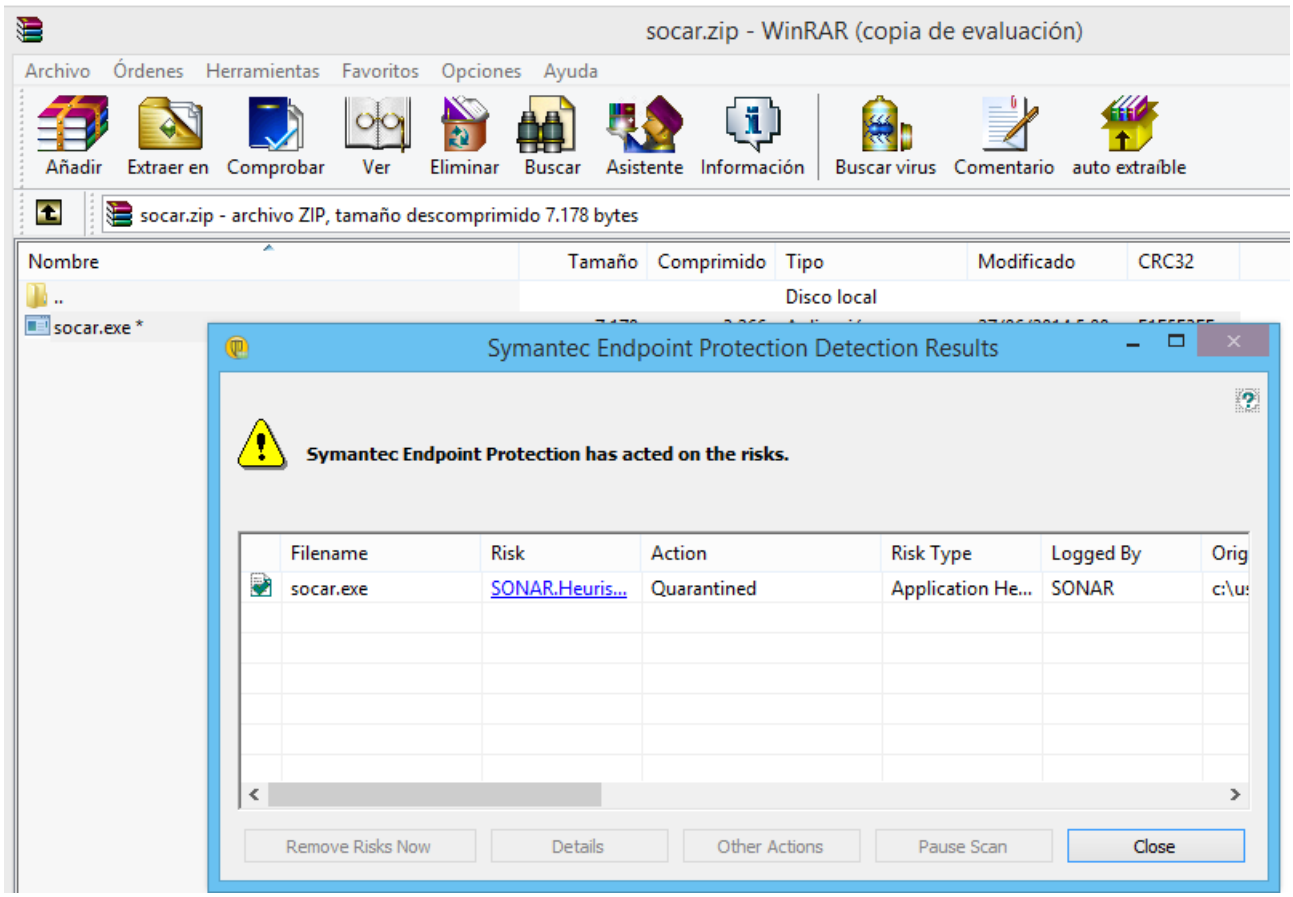


Ilustración 45: Test Protección heuristica

- Prevención de intrusiones

  Para comprobar el motor de IPS es preciso forzar un comportamiento que no se corresponda con el fin de una determinada aplicación de red o web. Para ello, se procede a renombrar un ejecutable como imagen y es subido a un servidor web, con ruta:

  http://10.232.73.5/portalaljarafe/images/pruebatest.gif

  Tratamos de abrir dicha URL y vemos que nos bloquea la conexión, ademas de generar un evento de dicho motor en el agente SEP

Ilustración 46: Error Web IPS

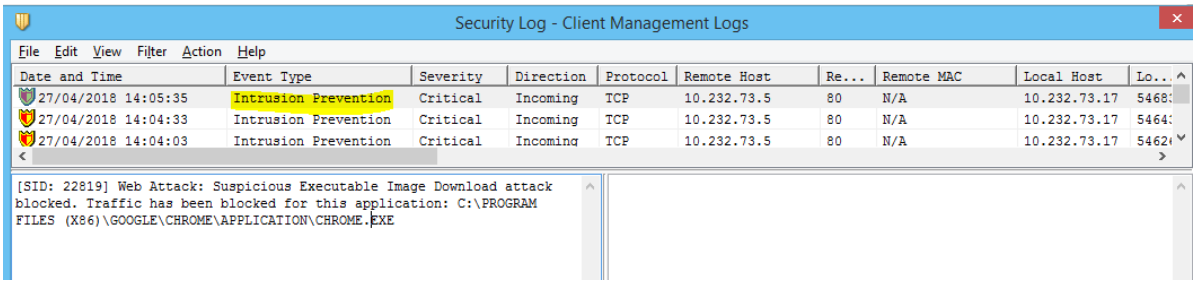


Ilustración 47: Test motor IPS

11. Desempeño

Una vez desplegada la plataforma y configuradas las políticas, las siguientes tareas están relacionadas con la monitorización de las funciones de seguridad que aportan un EPP. Estas funciones precisan un seguimiento continuo, dado que la seguridad no es un estado sino un proceso, el cual requiere de la definición de acciones y tareas que la garanticen.

El seguimiento al estado de la seguridad se enfoca desde 2 visiones:

- Reactiva: Mediante la supervisión de los reportes de estado y la mitigación de las amenazas encontradas.
- Proactiva: Revisión de boletines de seguridad y cumplimiento de recomendaciones.

11.1. Reportes

La revisión de estado de la consola se puede llevar a cabo mediante dos técnicas:

- Logs de estado.
- Reportes.

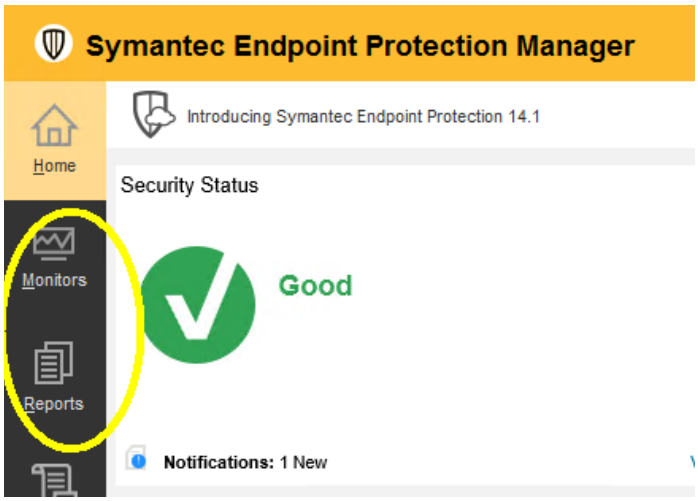


Ilustración 48: Tipos de informes

Los Logs son informes que permiten una mayor granularidad e interactividad, es por ello que son la mejor opción cuando precisamos ver la actividad de nuestros clientes para realizar una investigación sobre sus eventos.

Los reportes permiten un mayor nivel de datos estadísticos generales de la consola y tienen la características de poder ser programables, para tenerlos disponibles en el momento preciso.

Conforme a estas diferencias, podemos estimar que para un trabajo programado semanal de revisión, la opción correcta son los reportes.

La revisión de la consola se centrara en el seguimientos de los siguientes informes:

- Análisis de Riesgos por tecnología de detección
- Ataques. Top de equipos atacados
- Ataques. Top de equipos atacantes
- Clientes. Versión del Agente
- Clientes. Versión de Firmas
- Equipos sin agente de SEP

a) Análisis de Riesgos por tecnología de detección

Este informe nos ayuda a identificar la actividad de protección en cada una de las capas de Antivirus. Podemos identificar vulnerabilidades en nuestros endpoints que están tratando de ser explotadas por equipos remotos.

Lo combinaremos con los informes de origen y destino de los ataques para localizar las ips atacantes.

La ruta para ejecutar este informe es `Reports -> quick reports->Risk->Risk distribution by Protection Technology`, y los parámetros de ejecución se muestran a continuación:

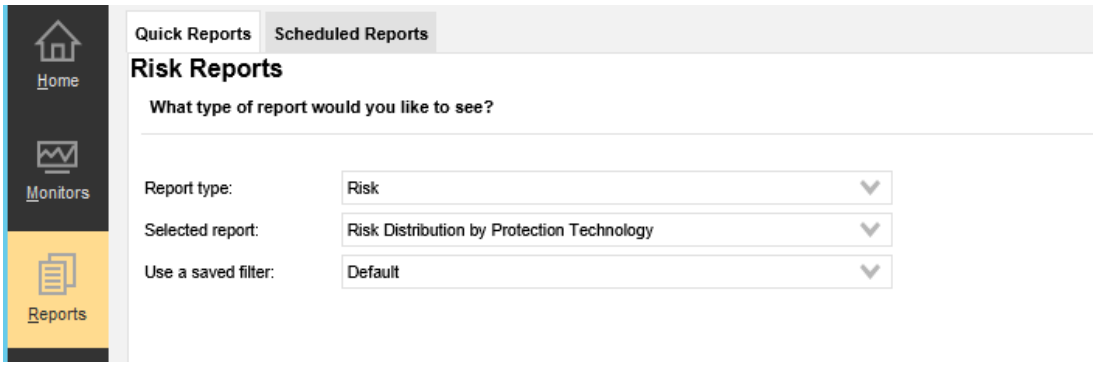


Ilustración 49: Reporte de riesgos por tecnología de protección

En los parámetros de selección, elegiremos `Past week`, para obtener los resultados de la última semana.

Podemos comprobar, en la cabecera del informe, en este caso, que el IPS es la capa que está registrando la mayor parte de la actividad de detección y remediación.

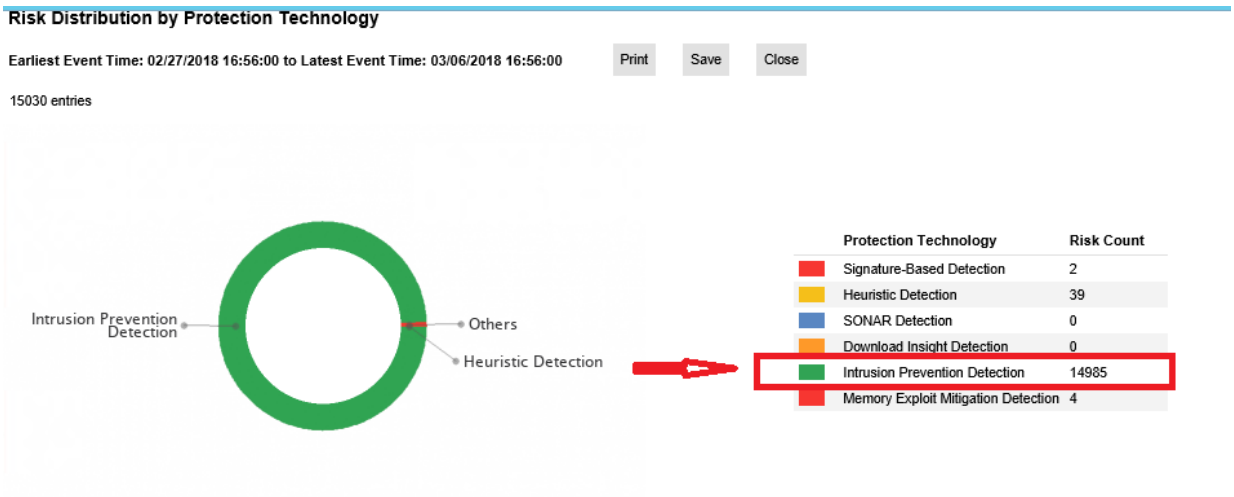
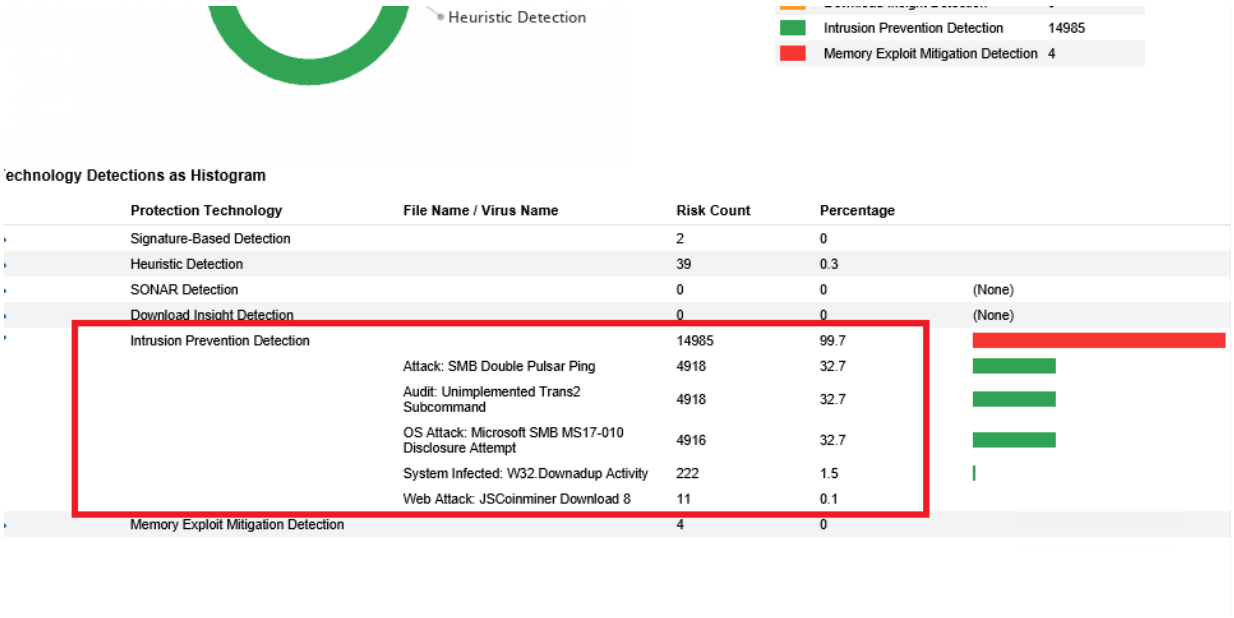


Ilustración 50: Distribución del riesgo

En el detalle del informe tendremos el detalle de los ataques interceptados por el IPS:



Protection Technology	File Name / Virus Name	Risk Count	Percentage	
Signature-Based Detection		2	0	
Heuristic Detection		39	0.3	
SONAR Detection		0	0	(None)
Download Insight Detection		0	0	(None)
Intrusion Prevention Detection		14985	99.7	
	Attack: SMB Double Pulsar Ping	4918	32.7	
	Audit: Unimplemented Trans2 Subcommand	4918	32.7	
	OS Attack: Microsoft SMB MS17-010 Disclosure Attempt	4916	32.7	
	System Infected: W32.Downadup Activity	222	1.5	
	Web Attack: JSCoinminer Download 8	11	0.1	
Memory Exploit Mitigation Detection		4	0	

Ilustración 51: Detalle del riesgo

Conociendo el tipo de ataques que está interceptando el IPS, podemos analizar las vulnerabilidades que tratan de explotar estos ataques, y a partir de aquí, determinar las acciones a realizar sobre nuestros endpoints, como:

- Actualizaciones del agente de AV o firmas.
- Actualizaciones de seguridad del SO.
- Actualizaciones de componentes del SO.

b) Ataques. Top de equipos atacados

Este reporte puede ser revisado desde la pantalla principal, en ella disponemos de un sumario de actividad donde encontramos esta información:

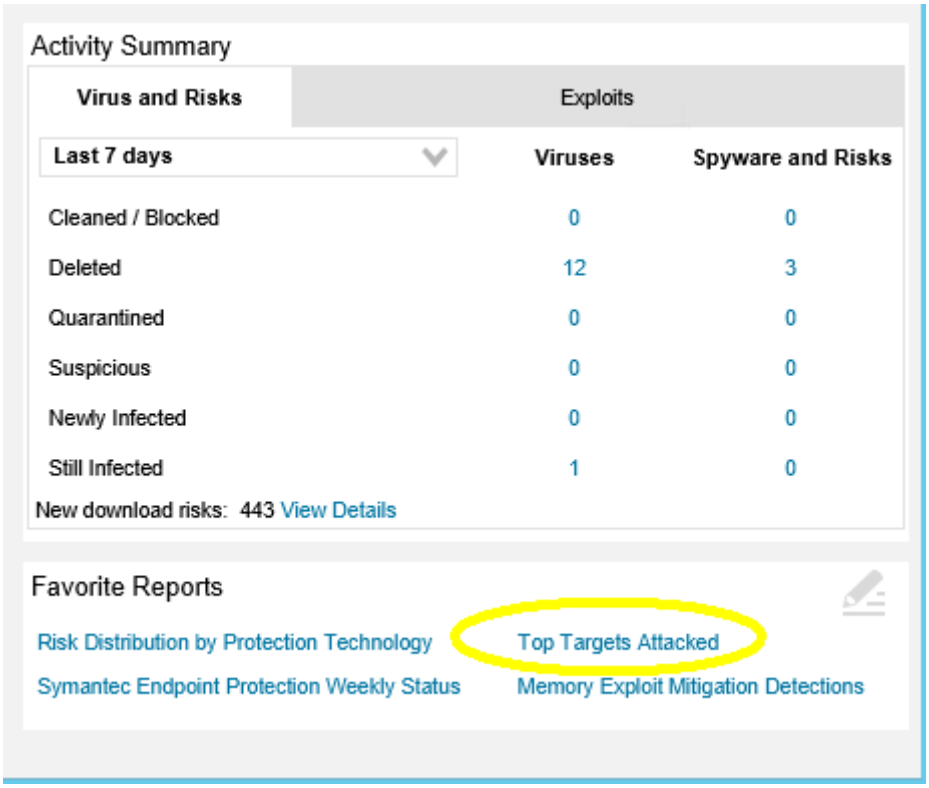


Ilustración 52: Reporte de equipos mas atacados

Este informe nos permitirá tener visibilidad de los equipos que reciben el mayor número de ataques. Es probable que los equipos listados en él tengan alguna vulnerabilidad no remediada, la cual, aunque pueda ser mitigada por el antivirus, convierte al equipo en objetivo de determinados tipos de malware. Los equipos protegidos y actualizados también pueden estar ubicados en un segmento de red en el que estén más expuestos a determinados ataques que contribuyan a aumentar su ratio de ataques recibidos.

Una vez obtenido el detalle de equipos atacados, se puede observar, que aun habiendo equipos que reciben más ataques que el resto, no podemos agrupar o segmentar estos equipos por encima del resto y de esta forma poder analizar una causa de esta situación. El informe de ataques por origen nos dará más información para realizar esta tarea.

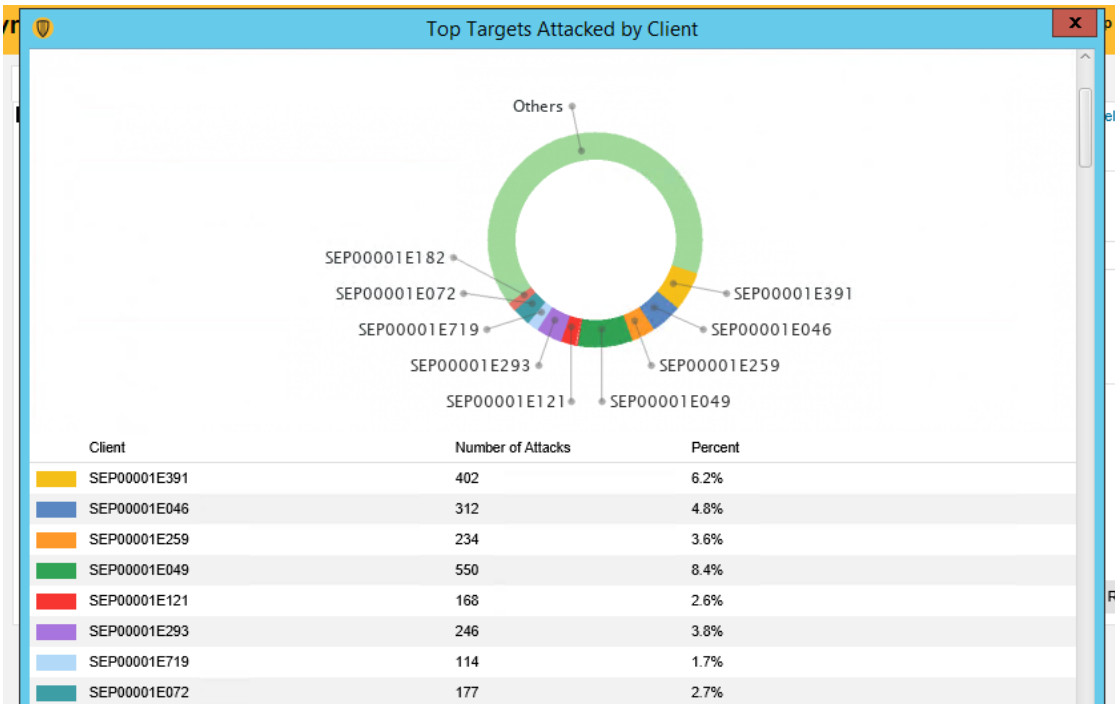


Ilustración 53: Top de equpos atacados

c) Ataques. Top de orígenes de los ataques

Este informe es útil para trabajar sobre el origen de los ataques, básicamente, aplicando un proceso de gestión de incidentes de seguridad.

Uno de los objetivos del tratamiento de esta información, es actuar como ente emisor de informes de riesgos, tal como realizan por ejemplo otros actores como AndalucíaCert, es por ello que si cruzamos la información de todos los emisores, encontremos información común a todos.

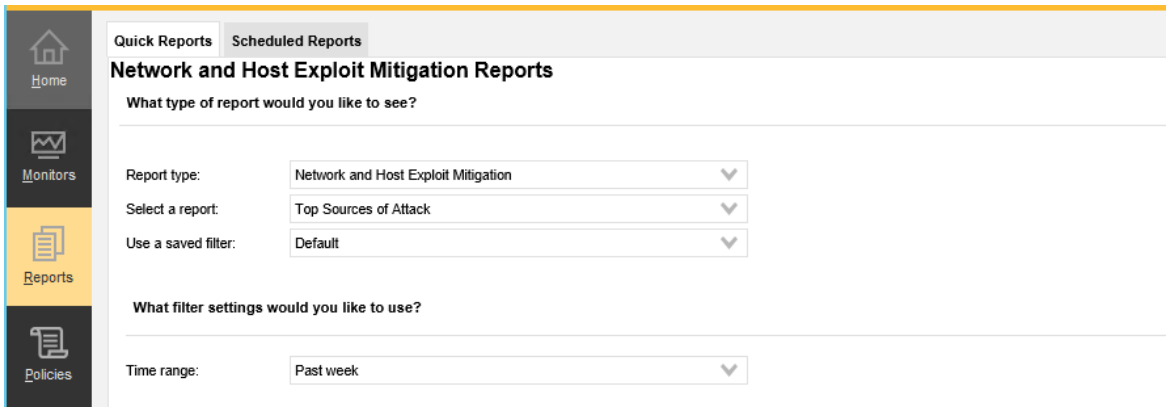


Ilustración 54: Reporte de mitigación de ataques

Los equipos origen de los ataques normalmente tienen una infección, que requiere ser solventada.

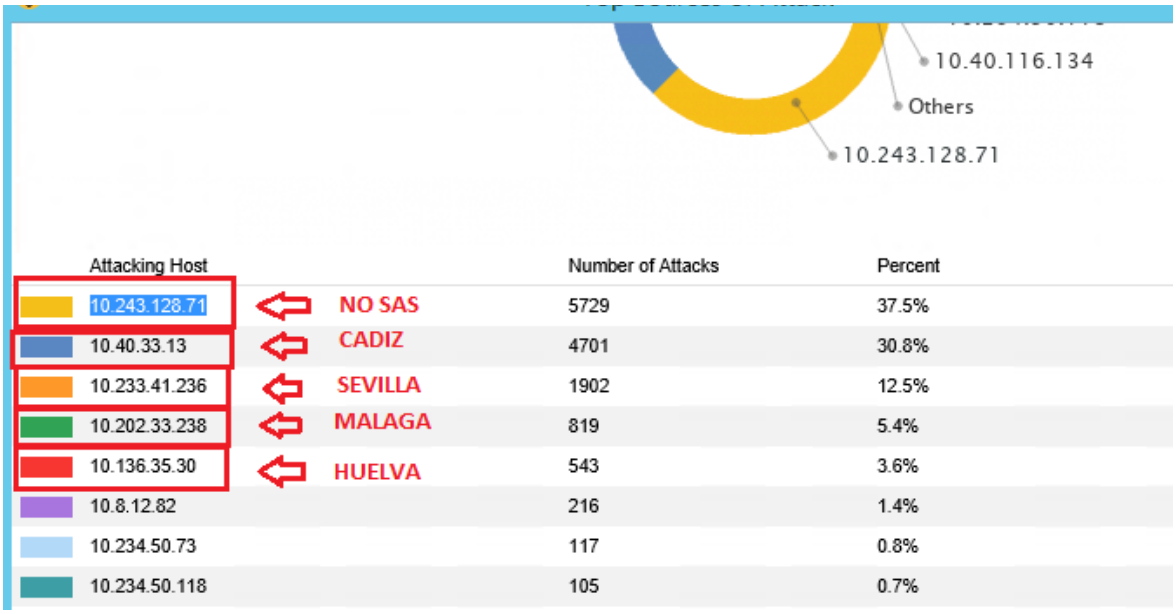


Ilustración 55: Análisis de atacantes

Podemos comprobar, si nos fijamos en los primeros 5 equipos origen de ataques, como tenemos:

- Equipos que están en direccionamiento no SAS (Servicio Andaluz de Salud)

- Equipos en direccionamiento SAS
    - Pertenecientes a nuestra provincia.
    - Pertenecientes a otras provincias.

En este, caso, aplicaremos un proceso de gestión de incidentes de seguridad para desencadenar las actuaciones necesarias para la remediación de los equipos origen de los ataques, o bien la mitigación de la amenaza, en el caso de equipos fuera del direccionamiento SAS.

Para obtener un mayor detalle de los ataques, nos apoyaremos en la sección `Monitors->Logs`.

d) Clientes. Versión del Agente

La versión del agente es un factor a tener en cuenta en el desarrollo de las políticas aplicadas y las funciones de protección disponibles, por ejemplo una versión antigua puede no tener la función de firewall incluido en el cliente antivirus.

Mediante esta revisión se deberá realizar un mantenimiento preventivo de los agentes desplegados buscando la unificación a la versión 14 en todos los agentes desplegados. Existen versiones de sistema operativo, como windows xp, que no la soportan, esto nos generara una excepción en este sentido.

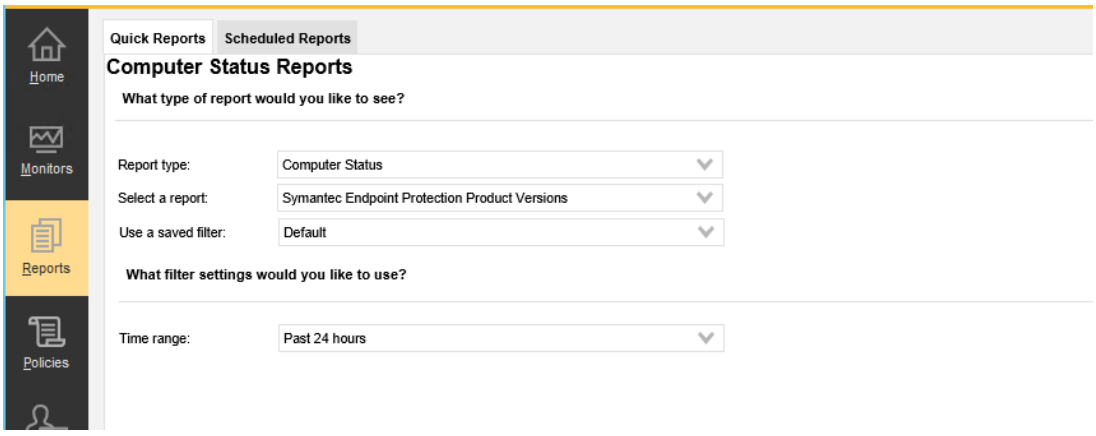
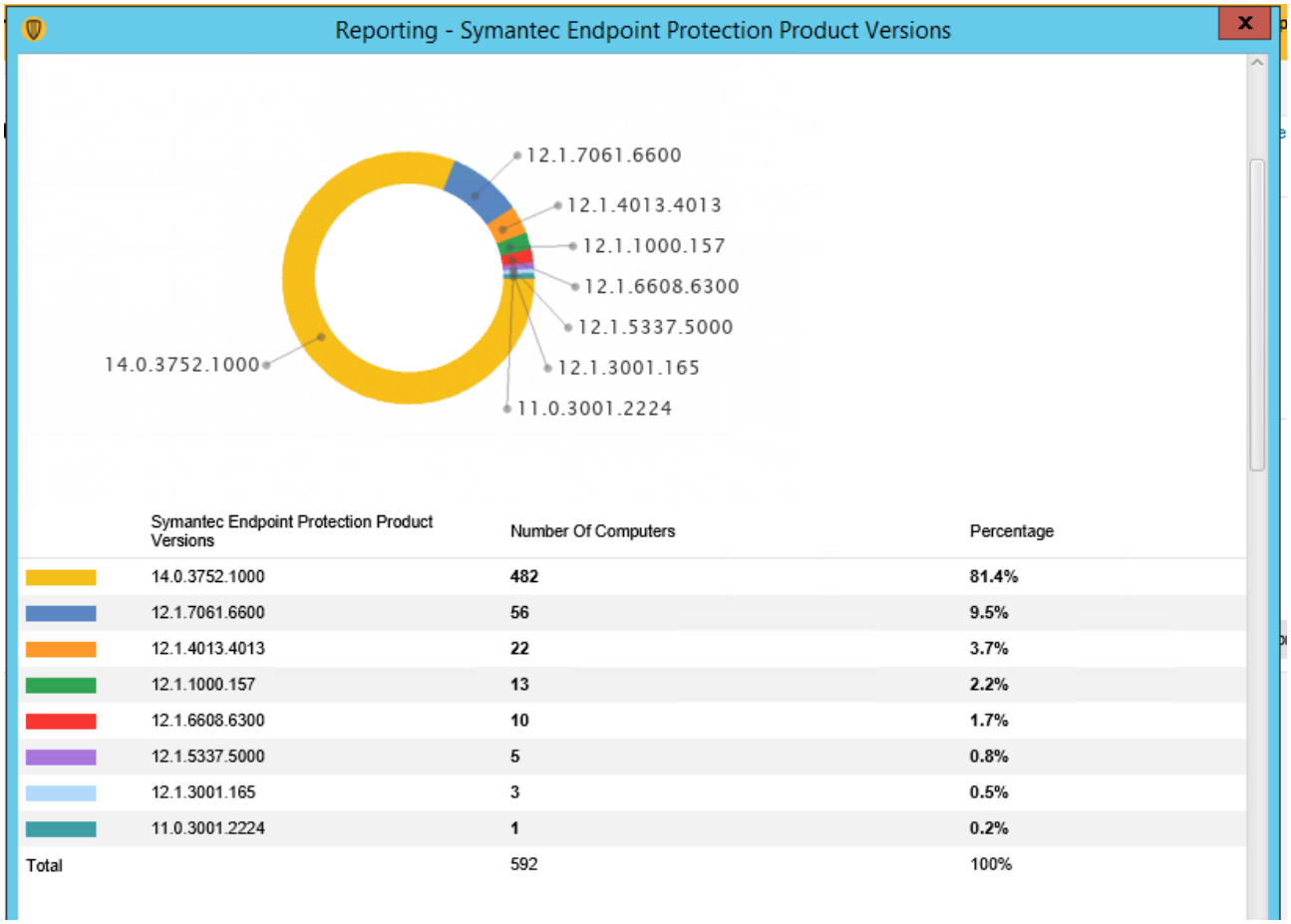


Ilustración 56: Reporte versiones agente



Symantec Endpoint Protection Product Versions	Number Of Computers	Percentage
14.0.3752.1000	482	81.4%
12.1.7061.6600	56	9.5%
12.1.4013.4013	22	3.7%
12.1.1000.157	13	2.2%
12.1.6608.6300	10	1.7%
12.1.5337.5000	5	0.8%
12.1.3001.165	3	0.5%
11.0.3001.2224	1	0.2%
Total	592	100%

Ilustración 57: Despliegue de versiones de agente

e) Clientes. Versión de Firmas

La version de firmas es un componente del cliente antivirus que permite una actualización continua de las diferentes tecnologías de detección incluidas en el producto.

Symantec libera diariamente varias versiones de firmas, podemos comprobar la última actualización en la web:
https://www.symantec.com/es/mx/security_response/definitions.jsp

El control de las versiones desplegada dependerá de la frecuencia en la descarga a la consola SEPM de las firmas, o bien en el servidor de LiveUpdate desplegado, junto con la frecuencia de conexión del cliente solicitando actualizaciones.

Con esta planificación podemos estimar informes que nos indiquen en que estado de actualización se encuentra nuestros clientes:

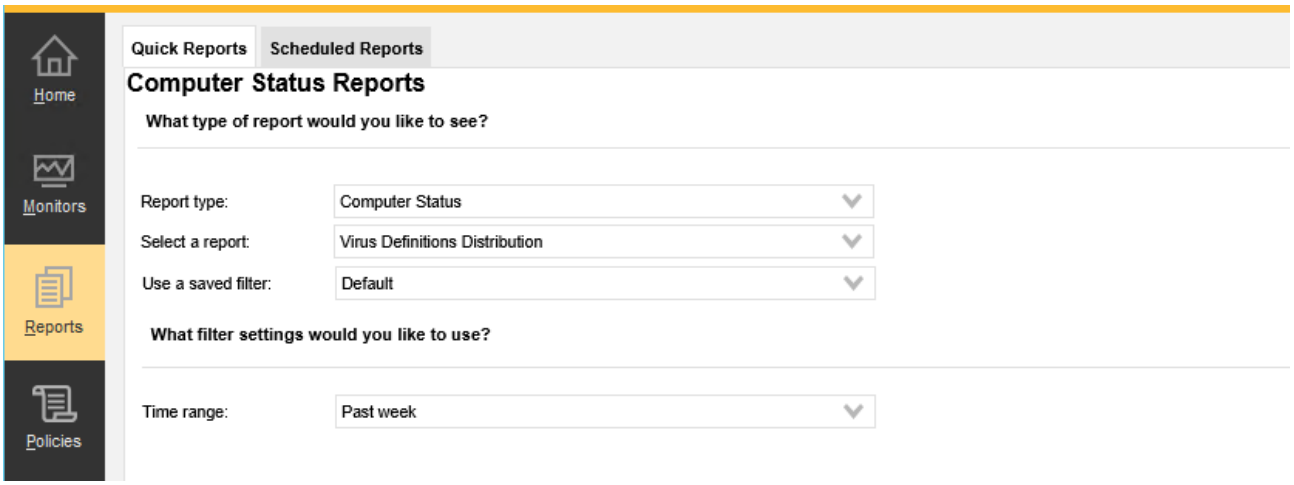
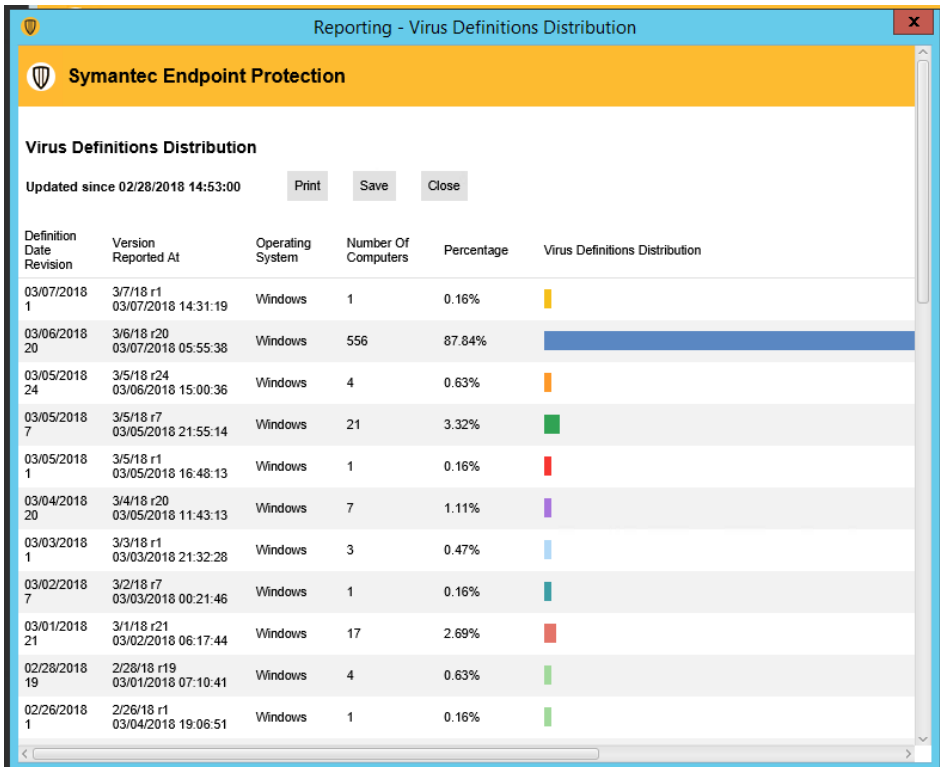


Ilustración 58: Reporte de firmas antivirus

Los equipos sin las definiciones correctas pueden ser objetivos de los ataques y debemos regular tareas para corregir su situación:



Definition Date Revision	Version Reported At	Operating System	Number Of Computers	Percentage	Virus Definitions Distribution
03/07/2018 1	3/7/18 r1 03/07/2018 14:31:19	Windows	1	0.16%	
03/06/2018 20	3/6/18 r20 03/07/2018 05:55:38	Windows	556	87.84%	
03/05/2018 24	3/5/18 r24 03/06/2018 15:00:36	Windows	4	0.63%	
03/05/2018 7	3/5/18 r7 03/05/2018 21:55:14	Windows	21	3.32%	
03/05/2018 1	3/5/18 r1 03/05/2018 16:48:13	Windows	1	0.16%	
03/04/2018 20	3/4/18 r20 03/05/2018 11:43:13	Windows	7	1.11%	
03/03/2018 1	3/3/18 r1 03/03/2018 21:32:28	Windows	3	0.47%	
03/02/2018 7	3/2/18 r7 03/03/2018 00:21:46	Windows	1	0.16%	
03/01/2018 21	3/1/18 r21 03/02/2018 06:17:44	Windows	17	2.69%	
02/28/2018 19	2/28/18 r19 03/01/2018 07:10:41	Windows	4	0.63%	
02/26/2018 1	2/26/18 r1 03/04/2018 19:06:51	Windows	1	0.16%	

Ilustración 59: Listado de distribución de firmas

f) Equipos sin agente de SEP

La detección de equipos sin protección de antivirus es una de las actividades más importantes que debemos tener en mente. La presencia en nuestra red de este tipo de elementos supone una amenaza para nuestros puestos de trabajo.

SEPM dispone de la función “unmanaged detector” que permite activar cualquier endpoint para que detecte equipos no gestionados en su segmento de red.

La recomendación es emplear al menos un “unmanaged detector” por segmento de red. Este equipo va a inspeccionar las tramas ARP, comparando con la tabla de endpoints gestionados por SEPM, para identificar equipos que no estén en la consola. Los resultados de la detección se registrarán en el log de la consola SEPM, para su posterior supervisión. Esta tarea es compatible con la función de GUP por lo que tendremos que analizar el despliegue de estos servicios en los segmentos de red necesarios.

Es importante indicar que el detector realiza su función mediante el envío de paquetes broadcast no rutables, por lo que es importante definir en que redes desplegaremos el servicio.

A continuación se detalla como activar endpoints para detectar equipos no gestionados por la consola SEPM (https://support.symantec.com/en_US/article.HOWTO80763.html)

1. En la consola, seleccionar `Clientes`
2. Seleccionar el grupo que contiene el cliente que queremos activar como `“unmanaged detector”`
3. Botón derecho sobre el equipo, y marcamos `“enable as unmananged detector”`
4. Si queremos configurar excepciones, seleccionaremos `“Configure unmanaged detector”`

   4.1. En el cuadro de dialogo, podremos añadir las excepciones.

Visualizar los equipos no gestionados detectados por el unmanaged detector:

1. En la sección `Home` de la consola, sección `Security Status`, seleccionar `View Details`.

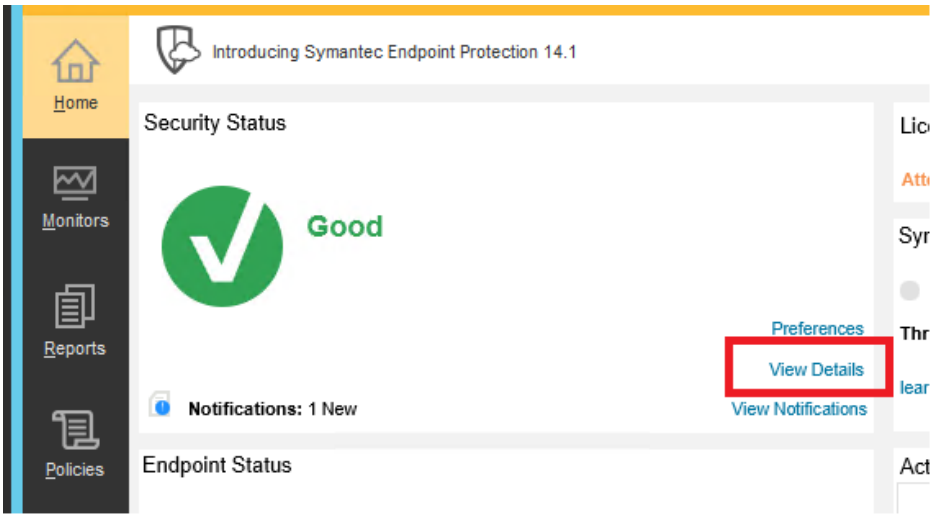


Ilustración 60: Reporte de equipos no gestionados

2. En el cuadro de dialogo de detalles, navegar hasta la tabla `Unknown Device Failures`

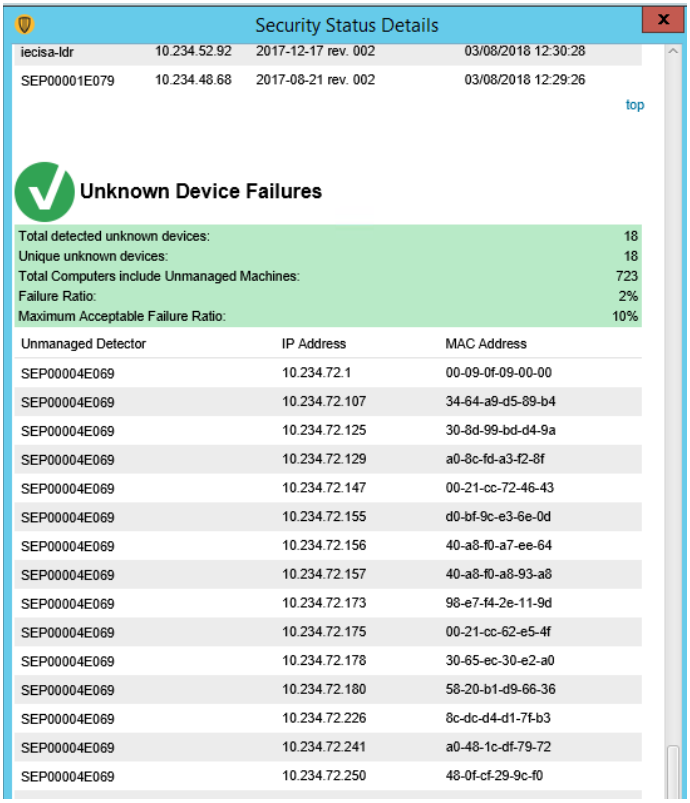


Ilustración 61: Listado de equipos no gestionados

Como podemos observar en la lista, tenemos una serie de dispositivos que se han detectado como no protegidos por SEPM. Para cada uno de ellos debemos desencadenar las acciones necesarias para instalar la protección de AV, según el proceso de Despliegue de Agentes.

11.2. Proactividad

Cualquier tipo de malware suele proceder a explotar vulnerabilidades en el sistema cliente para proceder a realizar sus funciones de ataque o distribución. Es una tarea del departamento de TI encargado de la seguridad de la red, el seguimiento y aplicación de recomendaciones que desde los proveedores de aplicaciones y sistemas operativos se realicé. También distintos Gobiernos han impulsado políticas publicas entorno a la seguridad de la información, creando observatorios públicos cuya misión es la alerta temprana de fuentes de riesgo entorno a la ciber-seguridad.

En España desde el Gobierno se dispone *"la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f)"* (Centro Criptológico Nacional, 2016, p.3), en esta guía llamada Esquema Nacional de Seguridad serán encontradas distintas pautas para implementar una metodología de ciberseguridad.

Desde la Organización se relazara un procedimiento de proactividad basado en los reportes anteriormente especificados, los cuales nos generaran los siguientes indicadores:

- Riesgos detectados

  Recuento del numero de equipos que generan ataques

- Incumplimiento de versión 14

  Recuento de equipos compatibles con la versión Antivirus establecida, pero no actualizados a la misma, versión 14 aplica a equipos con sistema operativo >=Windows7

- Incumplimiento de versión 12

Recuento de equipos compatibles con la versión Antivirus establecida, pero no actualizados a la misma, versión 12 aplica a equipos con sistema operativo WindowsXP

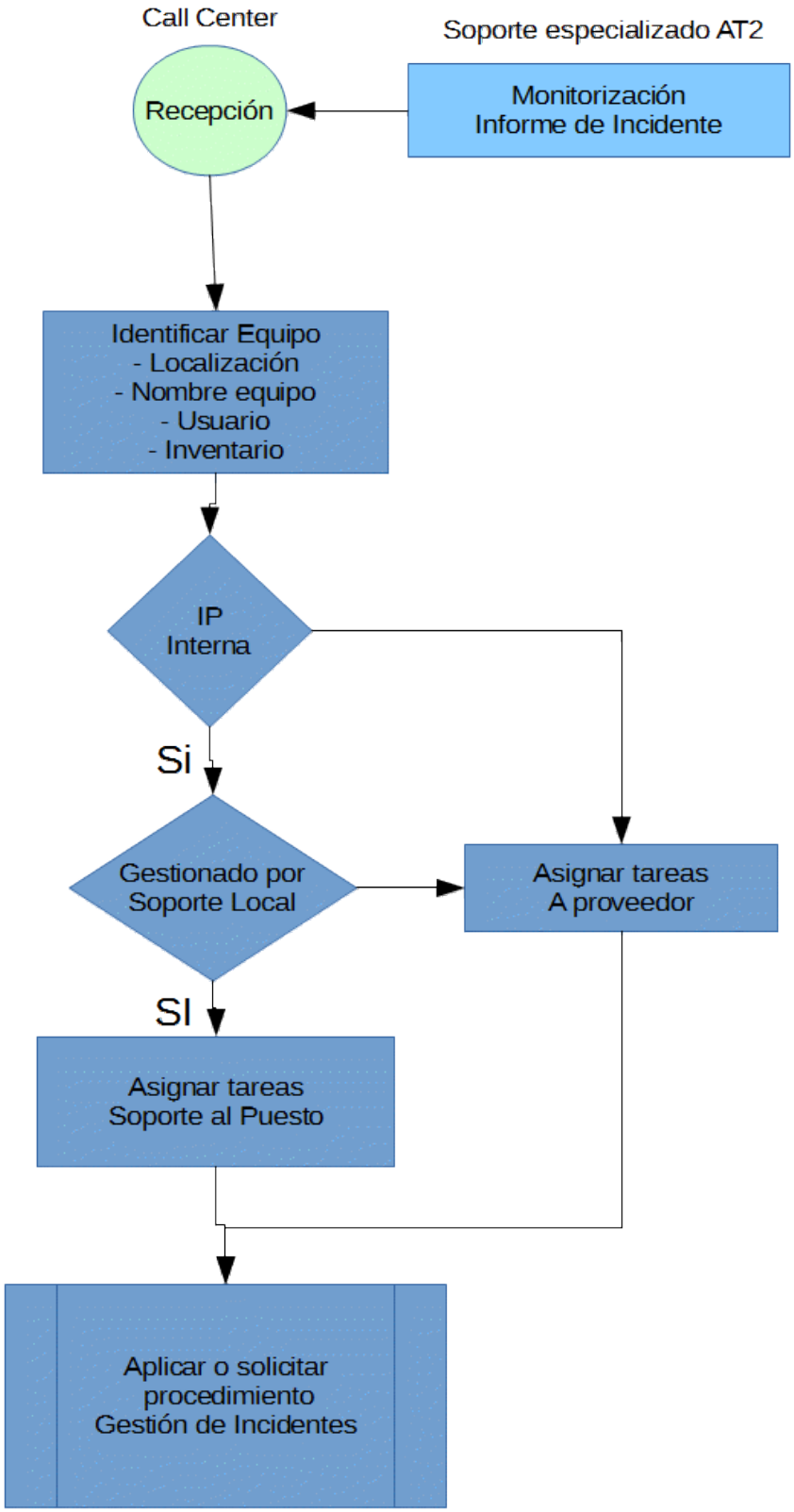
- Firmas desactualizadas

  Numero de equipos con un fichero de firma obsoleto, definido como obsoleto un fichero de firmas con una antigüedad superior a 3 días.

- Equipos sin protección Antivirus

  Equipos que no tienen instalado el agente SEP

El flujo de estas tareas desencadenan un procedimiento de “gestión de incidentes”, que podemos ver esquemáticamente en el siguiente flujo de tareas:


Call Center
Soporte especializado AT2
Recepción
Monitorización
Informe de Incidente
Identificar Equipo
- Localización
- Nombre equipo
- Usuario
- Inventario
IP
Interna
Si
Gestionado por
Soporte Local
Asignar tareas
A proveedor
SI
Asignar tareas
Soporte al Puesto
Aplicar o solicitar
procedimiento
Gestión de Incidentes

a) Gestión de incidentes

Para la identificación del equipo se procede a localizar el host en la consola SEPM y se revisan los datos obtenidos por el agente, los pasos a seguir:

- Búsqueda del host

  Desde la consola SEPM, se dispone de un buscador de clientes, en el cual es posible especificar distintos campos de búsqueda, uno de los valores que obtenemos en los informes son el campo IP:

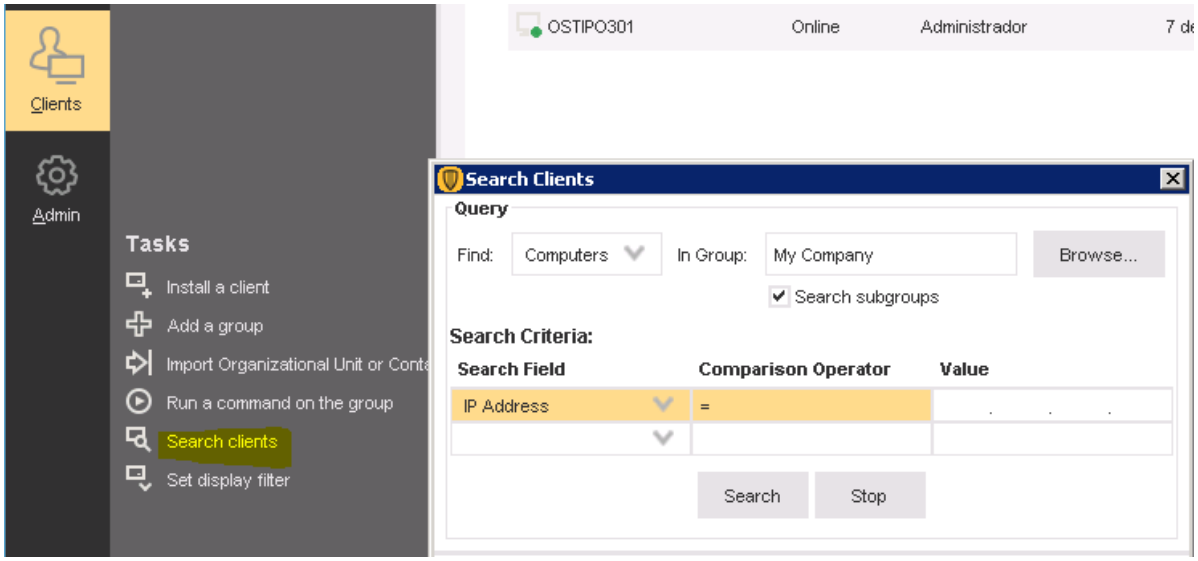


Ilustración 62: Búsqueda de clientes

- Recolección de información del cliente

  Una vez localizado, la consola SEPM nos ofrece obtener las propiedades del agente, con lo que se obtienen la información precisa en cuanto a identificación del equipo, usuario, ubicación, etc. Los datos mas importantes, ademas de los logísticos, son los que aplican al desempeño del propio antivirus, en el cual podemos ver la versión del cliente y su estado de actualización.

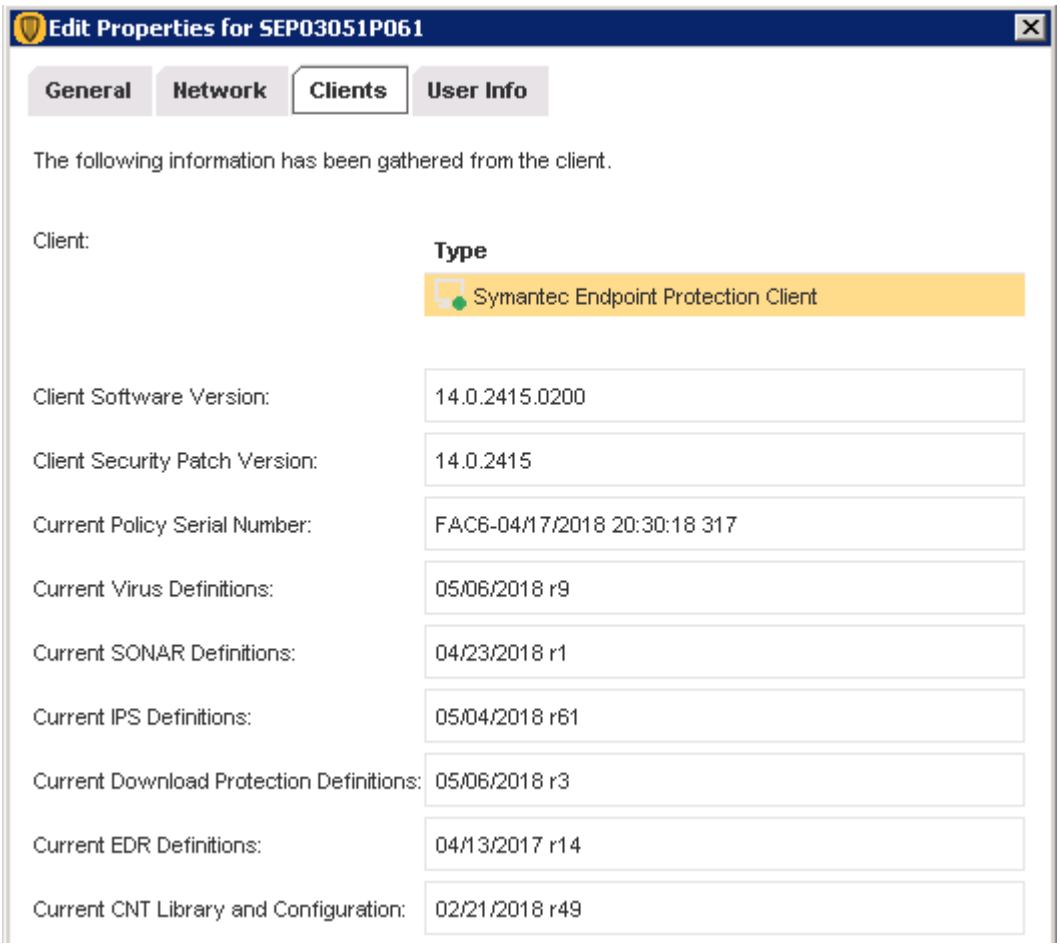


Ilustración 63: Información del agente SEP

- Cumplimiento de requisitos

  Con la información obtenida, se debe realizar una revisión de cumplimiento por parte del cliente. La información que desde la consola SEPM se puede remediar son tanto las versiones del cliente como su actualización de firmas.

  La actualización del cliente antivirus es posible realizar la con el mismo procedimiento, ya indicado, del despliegue de clientes, a la vez que la actualización de firmas se puede realizar desde la propia consola o bien realizando una descarga actualizada en la web de Symantec y forzando su ejecución en el cliente SEP: https://www.symantec.com/es/mx/security_response/definitions.jsp

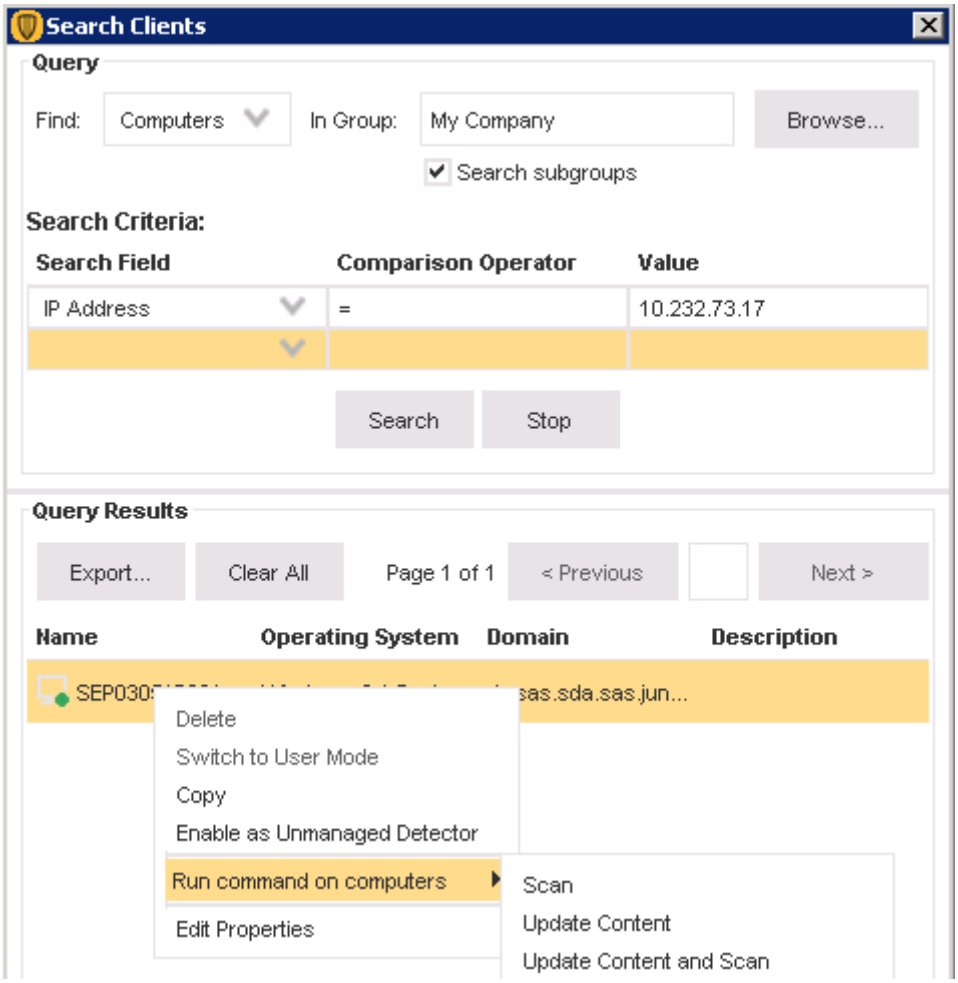


Ilustración 64: Actualización de contenido en SEP

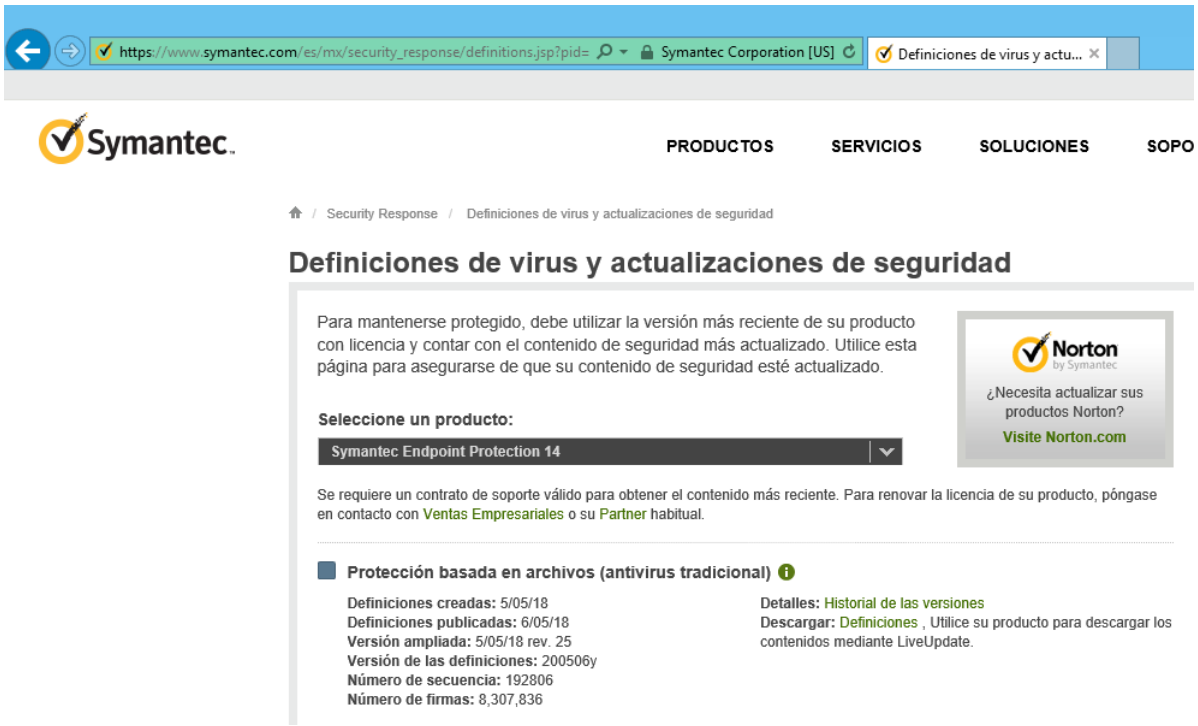


Ilustración 65: Descarga de contenido

Complementaria a estas tareas relacionadas con el antivirus, también son la definición y cumplimiento de despliegue de los parches de seguridad del sistema operativo del cliente.

- Remediación

  La propia configuración del antivirus realiza un análisis sobre los ficheros usados por el usuario, a la vez que incluye programaciones diarias y semanales sobre el sistema de fichero del equipo. Desde la consola SEPM es posible forzar una búsqueda de amenazas tras actualizar las firmas del antivirus.

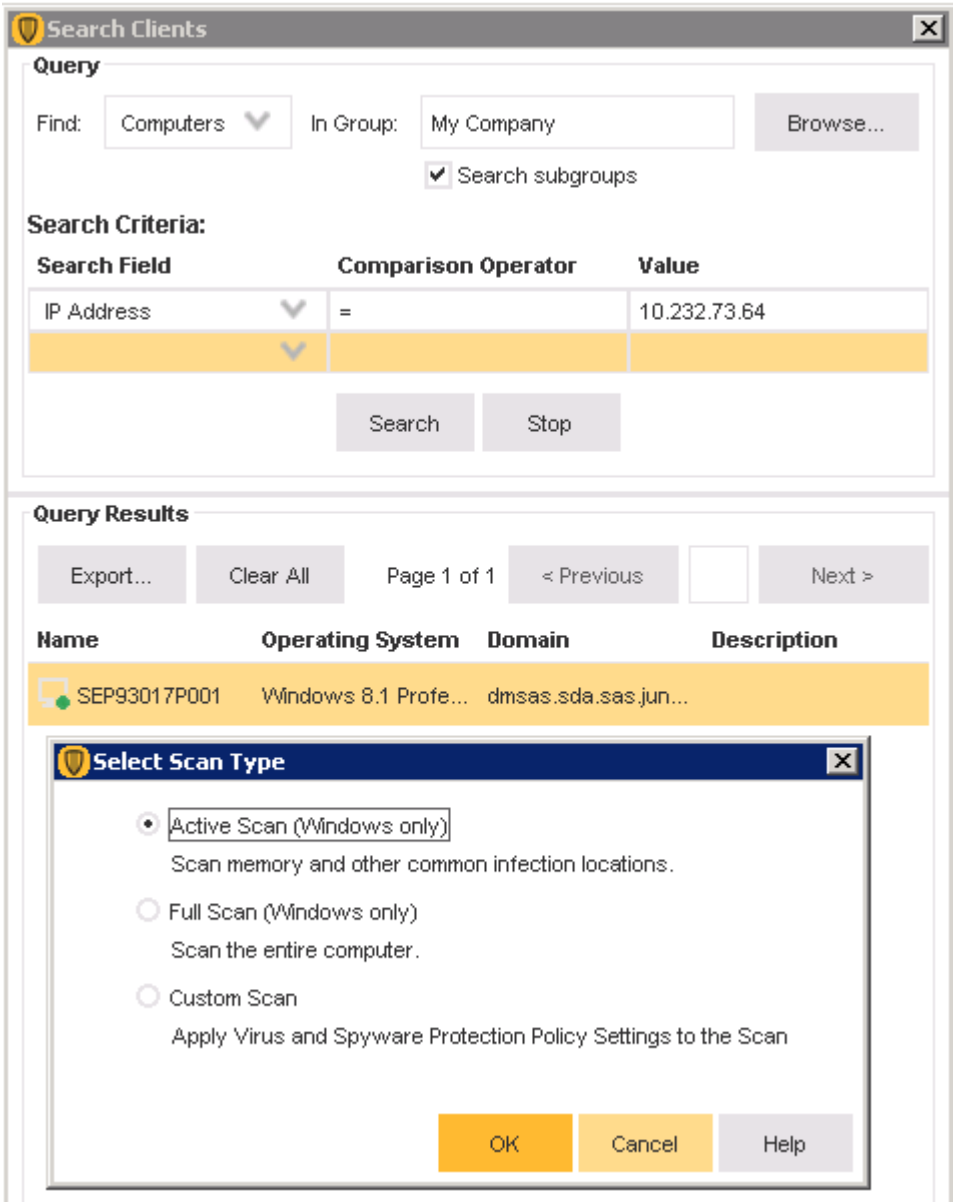


Ilustración 66: Remediación desde la consola SEPM

Podemos comprobar el estado de estas tareas desde la ventada de estado en el apartado Monitors:

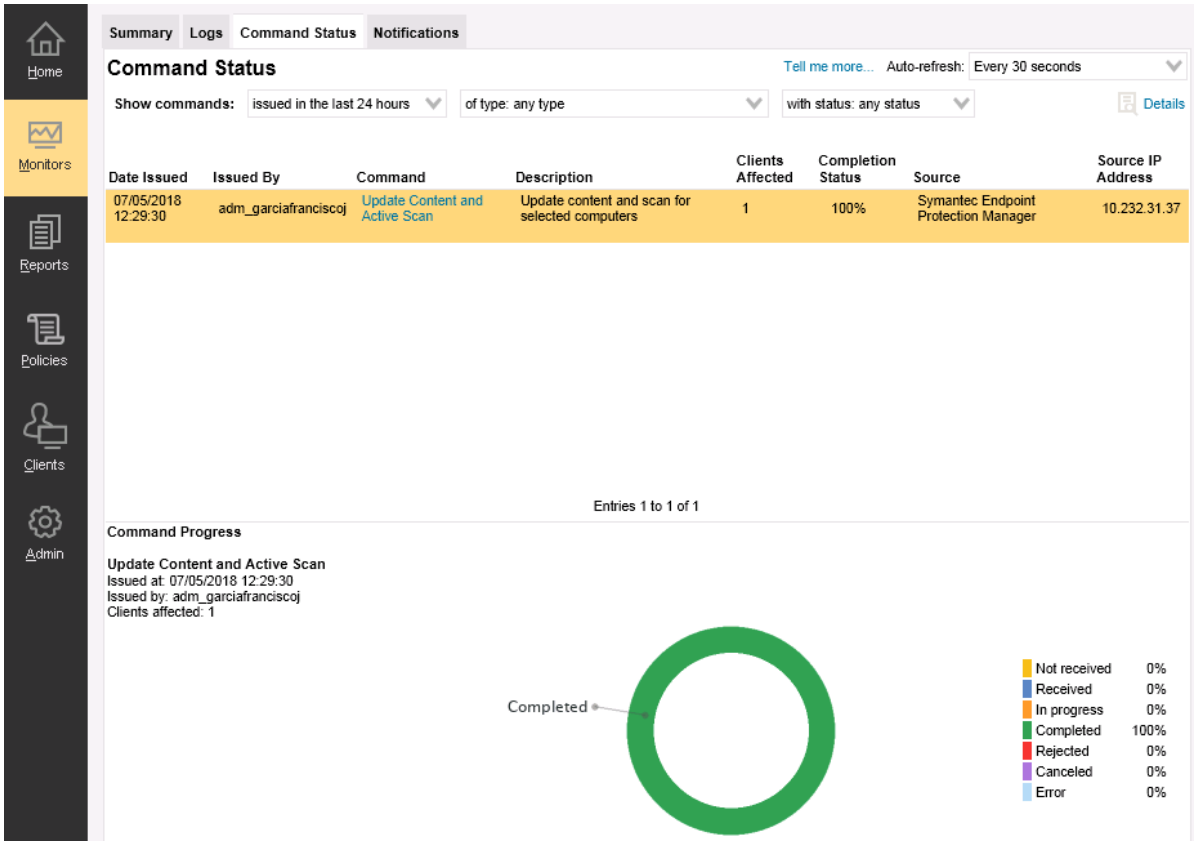


Ilustración 67: Monitorización de tareas sobre clientes

Desde las herramientas de Symantec, se provee de una herramienta que permite realizar un análisis y recolección de información del equipo infectado para poder aplicar un método de limpieza acorde al tipo de infección detectada. Esta aplicación se conoce como Symantec Diagnostic Tool (SymDiag) y es preciso descarga la última versión desde la web:
https://support.symantec.com/en_US/article.TECH170752.html

Esta aplicación precisa permisos de ejecución como administrador del equipo, a la vez que en ciertos análisis (root kits) precisa un reinicio del equipo, es por ello que estas tareas se realizaran in-situ por personal especializado del soporte de informática.

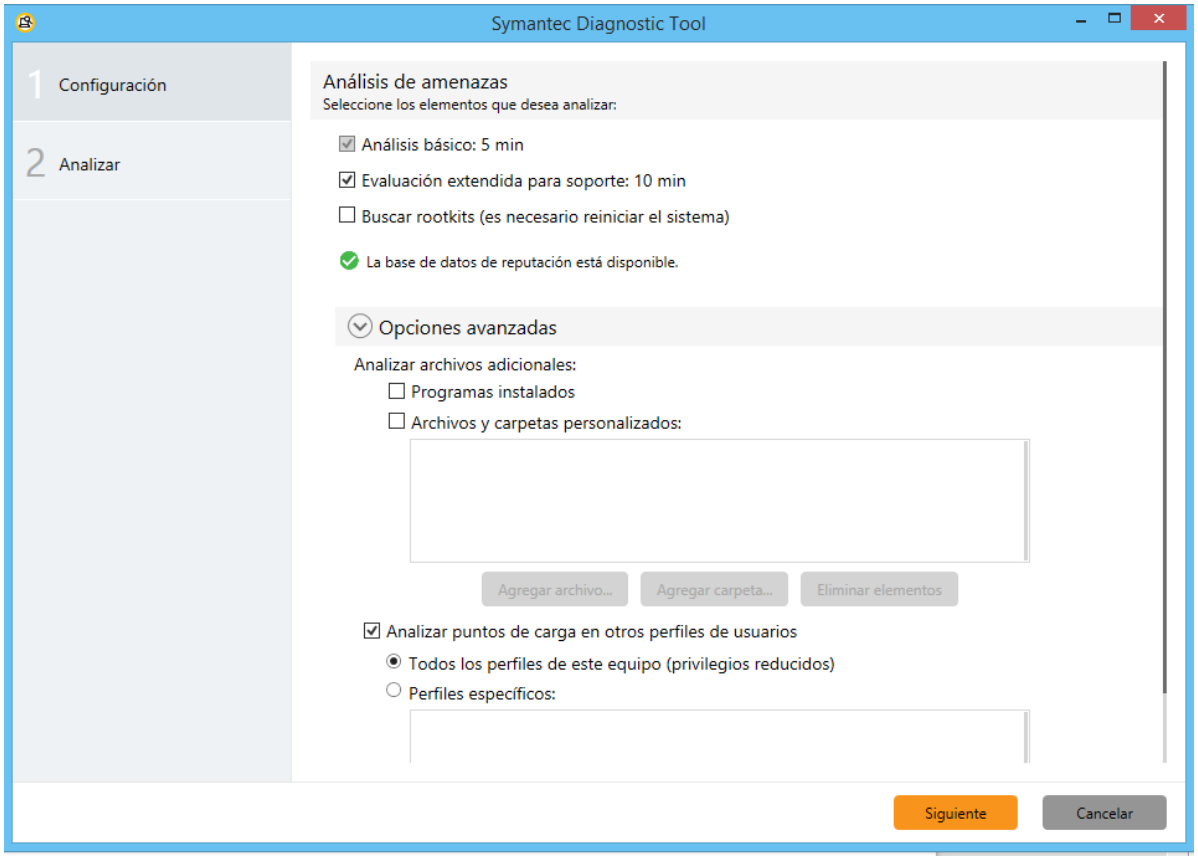


Ilustración 68: Symantec Diagnostic Tool

Finalmente, en el caso de que usando estos procesos no quedara solventando el incidente, mediante la propia SymDiag se genera un reporte que analizaría Symantec, como proveedor del sistema de antivirus, y se aplicarían las medidas indicadas por ellos.

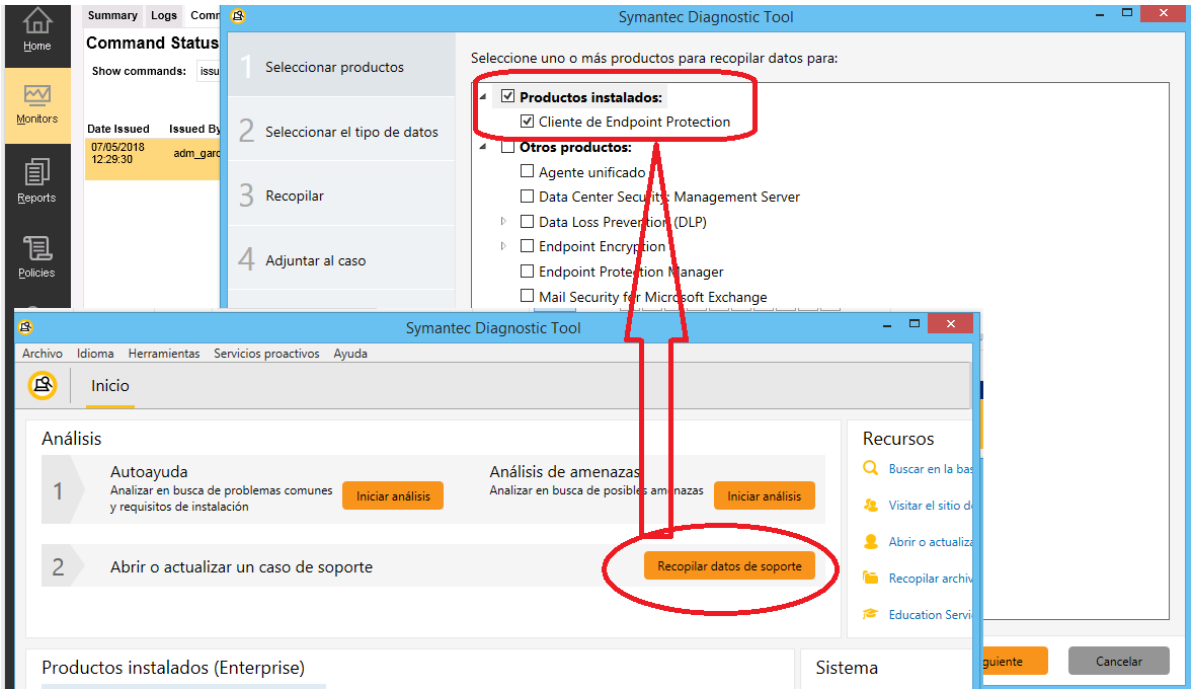


Ilustración 69: Abrir caso de soporte con Symantec

Es conveniente en esos casos aislar el riego (en caso de que sea posible) para ello desde la consola SEPM podemos aplicar una política de firewall que establece un estado de cuarentena sobre el host, permitiendo solo las comunicaciones con los servidores de actualización consola para realizar las acciones de remediación:

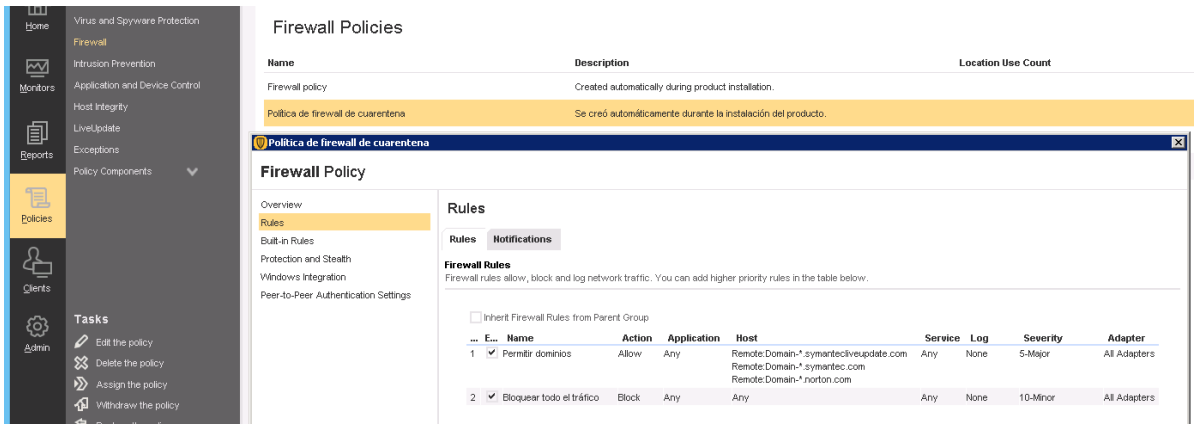


Ilustración 70: Política de aislamiento

11.3. Conclusiones

Cualquier compañía, grande o pequeña, se ve expuesta a distintas amenazas relacionadas con la ciberseguridad. En pequeñas empresas se pueden realizar tareas individuales en los distintos equipos, sin embargo en grandes compañía es necesario la implantación de distintas herramientas que permitan una protección centralizada que garanticen, sobre todo, un tiempo de respuesta razonable frente a ellos, *"los incidentes ocurrirán, solo desconocemos cuando"*.

Un EPP es solo una pieza de las necesarias para garantizar un entorno seguro en los sistemas de información, se ha de tener en cuenta que los ataques evolucionan, por lo tanto los medios y sistemas de protección también deben evolucionar con ellos, sin embargo el sistema EPP se convierte en la piedra angular en la que se apoyaran las demás herramientas, por ejemplo los NGFW (Next Generation Firewalls), por lo cual esta herramienta es la primera a implantar, y ayudara a medir los sistemas de seguridad existentes.

Tras el uso del sistema, se realizan un informe de desempeño del proyecto en base a la definición de reportes y seguimiento descrito en la memoria. Para esto se genera unos indicadores con los datos obtenidos en los siguientes puntos analizados:

- Riesgos detectados
- Incumplimiento de versiones de antivirus (distintas según sistema operativo).
- Equipos con protecciones desactualizadas
- Equipos sin protección Antivirus

Dicho informe se entrega a la Dirección de la Organización y permitirá, nos solo conocer tras la implantación del producto el estado actual del mismo, sino también aportar el desempeño del producto a lo largo del tiempo con la comparativa que se pueda realizar entre los distintos informes.

En dicho informe, que incluimos en este apartado, se refleja el estado inicial del proyecto, del cual destacamos que encontramos un parque con muchas amenazas, que ahora ya podrán ser analizadas y mitigadas por el propio antivirus mediante el plan de actuación definido en este proyecto, a la vez que ayudara a dimensionar los recursos y tiempo necesarios para ello.

Como conclusión final, vemos que la seguridad es un proceso que precisa herramientas, las cuales nos proporciona un visión de la situación y capacidad de adaptación frente a los nuevos problemas de seguridad que se generen a lo largo del ciclo.

Informe de indicadores del proyecto.

	Totales	Dis_Sevilla	Dis_Aljarafe	Dis_Norte	HUVR	AGSUR-HUVV	HUVM	AGSOSUNA
Riesgos detectados	5642	30	19	64	4454	434	438	203
Incumplimiento de Versión 14	54	0	0	0	24	10	15	5
Incumplimiento de Versión 12	2104	132	76	58	606	378	695	159
Firmas desactualizada	330	114	8	4	37	33	25	109
Equipos sin protección Antivirus	81	7	3	0	21	19	24	7

Tabla 11: Indicadores implantación Proyecto

12. ANEXO I

Tipología	Nombre	Descripción	Reducida	Estándar	Avanzada
Proactiva	Obligatoriedad de cliente de antivirus	Obligatoriedad de disponer de cliente de antivirus corporativo en todos los puestos cliente Windows.	Aplica	Aplica	Aplica
Proactiva	Escaneo de Red de equipos sin agente instalado	Planificación de escaneos de red por parte de Altiris y SEP para detectar clientes que no dispongan de software obligatorio instalado	Aplica	Aplica	Aplica
Reactiva	Configuración Escaneos programados	Parámetros que determinan el tipo de escaneo programado que debe ejecutarse sobre todos los equipos.	- Al menos 1 análisis completo semanal - Al menos 1 análisis activo diario. - Al menos Insight Level 1 (sensibilidad archivos maliciosos) - Escaneo de archivos remotos: NO	- Al menos 1 análisis completo semanal - Al menos 1 análisis activo diario. - Al menos 4 niveles de profundidad en ficheros comprimidos. - Al menos Insight Level 5 (sensibilidad archivos maliciosos) - Escaneo de archivos	- Al menos 1 análisis diario. - Al menos 4 niveles de profundidad en ficheros comprimidos. - Al menos Insight Level 5 (sensibilidad archivos maliciosos) - Escaneo de archivos remotos: SI

Tipología	Nombre	Descripción	Reducida	Estándar	Avanzada
				remotos: SI	
Reactiva	Acciones tras detección en escaneos programados	Acciones programadas que deben desencadenarse tras detección de malware y riesgos de seguridad tras escaneos programados.	- Detección Malware (1ª acción/2ª acción): Clean/Quarantine. - Detección Riesgos de seguridad (1ª acción/2ª acción): Quarantine / Leave alone (log only). - Detección Insight reputation: Quarantine / Leave alone (log only)	- Detección Malware (1ª acción/2ª acción): Clean/Quarantine. - Detección Riesgos de seguridad (1ª acción/2ª acción): Quarantine / Leave alone (log only). - Detección Insight reputation: Quarantine / Leave alone (log only)	- Detección Malware (1ª acción/2ª acción): Clean/Quarantine - Detección Riesgos de seguridad (1ª acción/2ª acción): Quarantine/Delete risk. - Detección Insight reputation: Quarantine / Leave alone (log only)
Proactiva	Configuración autoprotección	Parámetros que determinan la configuración que debe tener el sistema de autoprotección del antivirus.	- Inicio de autoprotect al inicio del equipo. - Habilitar risk-tracer - Escanear todo los tipos de ficheros. - Escanear riesgos de seguridad: NO - Escanear cuando un fichero es accedido o modificado: SI - Escanear ficheros en equipos remotos: NO	- Inicio de autoprotect al inicio del equipo. - Habilitar risk-tracer - Escanear todo los tipos de ficheros. - Escanear riesgos de seguridad: SI - Escanear cuando un fichero es accedido o modificado: SI - Escanear ficheros en equipos remotos: SI	- Inicio de autoprotect al inicio del equipo. - Habilitar risk-tracer - Escanear todo los tipos de ficheros. - Escanear riesgos de seguridad: SI - Escanear cuando un fichero es accedido o modificado: SI - Escanear ficheros en equipos remotos: SI
Proactiva	Acciones tras detección en autoprotección	Acciones programadas que deben desencadenarse tras	- Detección Malware (1ª acción/2ª acción): Limpieza/Cuarentena.	- Detección Malware (1ª acción/2ª acción): Limpieza/Cuarentena.	- Detección Malware (1ª acción/2ª acción): Limpieza/Cuarentena.

Tipología	Nombre	Descripción	Reducida	Estándar	Avanzada
		detección de malware y riesgos de seguridad mediante los mecanismos de autoprotección.	- Detección Riesgos de seguridad (1ª acción/2ª acción): Cuarentena/Leave Alone	- Detección Riesgos de seguridad (1ª acción/2ª acción): Cuarentena/Leave Alone	- Detección Riesgos de seguridad (1ª acción/2ª acción): Cuarentena/Leave Alone
Proactiva	Configuración de Protección en descargas	Parámetros que determinan la configuración que debe tener el sistema de protección de descargas.	- Activar Download Insight - Al menos Insight Level 1 (sensibilidad archivos maliciosos)	- Activar Download Insight - Al menos Insight Level 5 (sensibilidad archivos maliciosos)	- Activar Download Insight - Al menos Insight Level 5 (sensibilidad archivos maliciosos)
Proactiva	Acciones tras detección en descargas	Acciones programadas que deben desencadenarse tras detección de malware y riesgos de seguridad mediante los mecanismos de protección de descargas.	- Detección de descargas maliciosas(1ª acción/2ª acción): Cuarentena/Leave Alone - Mostrar las notificaciones de Insight en el ordenador infectado.	- Detección de descargas maliciosas(1ª acción/2ª acción): Cuarentena/Leave Alone - Mostrar las notificaciones de Insight en el ordenador infectado.	- Detección de descargas maliciosas(1ª acción/2ª acción): Cuarentena/Leave Alone - Mostrar las notificaciones de Insight en el ordenador infectado.
Proactiva	Configuración Protección Zero-Day (SONAR)	Parámetros que determinan la configuración del sistema proactivo de detección de	Configuración de SONAR: activado	Configuración de SONAR: activado	Configuración de SONAR: activado

Tipología	Nombre	Descripción	Reducida	Estándar	Avanzada
		vulnerabilidades de día cero y riesgos de seguridad.			
Proactiva	Acciones tras detección en Protección Zero-Day (SONAR)	Acciones programadas que deben desencadenarse tras detección de malware y riesgos de seguridad mediante los mecanismos de protección Zero-Day (SONAR).	- Detección Alto Riesgo: cuarentena - Detección Bajo Riesgo: log - Cambio de DNS detectado: bloquear (monitorizar en la 1ª fase) - Cambio de fichero hots detectado: bloquear (monitorizar en la 1ª fase) - Detección de comportamiento sospechoso riesgo alto: bloquear Detección de comportamiento sospechoso riesgo bajo: log"	- Detección Alto Riesgo: cuarentena. - Detección Bajo Riesgo: log - Cambio de DNS detectado: bloquear (monitorizar en la 1ª fase) - Cambio de fichero hots detectado: bloquear. (monitorizar en la 1ª fase) - Detección de comportamiento sospechoso riesgo alto: bloquear Detección de comportamiento sospechoso riesgo bajo: log"	- Detección Bajo Riesgo: log - Cambio de DNS detectado: bloquear (monitorizar en la 1ª fase) - Cambio de fichero hots detectado: bloquear (monitorizar en la 1ª fase) - Detección de comportamiento sospechoso riesgo alto: bloquear - Detección de comportamiento sospechoso riesgo bajo: bloquear
Proactiva	Configuración de Email-Autoprotect	Parámetros que determinan la configuración del	- Activar Email Auto-Protect - Activar Outlook Auto-	- Activar Email Auto-Protect Activar Outlook Auto-	- Activar Email Auto-Protect - Activar Outlook Auto-

Tipología	Nombre	Descripción	Reducida	Estándar	Avanzada
		sistema de escaneo de ficheros de correo electrónico.	Protect (DpC Escanear todos los tipos de ficheros)	Protect (DpC Escanear todos los tipos de ficheros) - Al menos 3 niveles de profundidad en ficheros comprimidos."	Protect (DpC) - Escanear todos los tipos de ficheros - Al menos 3 niveles de profundidad en ficheros comprimidos.
Proactiva	Acciones tras detección en Email-Autoprotect	Acciones programadas que deben desencadenarse tras detección de malware y riesgos de seguridad mediante los mecanismos de protección de correo electrónico.	- Detección Malware (1ª acción/2ª acción): Limpieza/Cuarentena. - Detección Riesgos de seguridad (1ª acción/2ª acción): Cuarentena/Leave Alone - Mostrar un notificación en el equipo infectado. - Añadir un warning en el correo"	- Detección Malware (1ª acción/2ª acción): Limpieza/Cuarentena. - Detección Riesgos de seguridad (1ª acción/2ª acción): Cuarentena/Leave Alone - Mostrar un notificación en el equipo infectado. - Añadir un warning en el correo"	- Detección Malware (1ª acción/2ª acción): Limpieza/Cuarentena. - Detección Riesgos de seguridad (1ª acción/2ª acción): Cuarentena/Leave Alone - Mostrar un notificación en el equipo infectado. - Añadir un warning en el correo"
Proactiva	Configuración de cuarentena	Parámetros que determinan la configuración de la cuarentena de ficheros infectados/sospechoso s.	- Tras actualización de nuevas definiciones de firmas: reparación silenciosa del fichero y restauración. - Borrado de ficheros en cuarentena tras 30		

Tipología	Nombre	Descripción	Reducida	Estándar	Avanzada
			días."		
Proactiva	Actualizaciones de definiciones y firmas	Política vinculada a la periodicidad de búsqueda de firmas, su actualización y su comportamiento.	- Programación de Live-Update: diaria - Mostrar mensaje de sistema (Centro de Seguridad de Microsoft) tras 3 días de obsolescencia de las firmas"	- Programación de Live-Update: cada 4 horas - Mostrar mensaje de sistema (Centro de Seguridad de Microsoft) tras 3 días de obsolescencia de las firmas	- Programación de Live-Update: cada 4 horas - Mostrar mensaje de sistema (Centro de Seguridad de Microsoft) tras 3 días de obsolescencia de las firmas
Proactiva	Logs	Política de información que debe recopilarse en los logs. Información a recopilar	- Análisis cancelado - Análisis iniciado - Análisis parado - Fallo de reparación - Cliente sin definiciones de virus - Restablecimiento de las definiciones de virus - Antivirus instalado - Error ejecutando servicios	- Análisis cancelado - Análisis iniciado - Análisis parado - Fallo de reparación - Cliente sin definiciones de virus - Restablecimiento de las definiciones de virus - Antivirus instalado - Error ejecutando servicios	- Análisis cancelado - Análisis iniciado - Análisis parado - Fallo de reparación - Cliente sin definiciones de virus - Restablecimiento de las definiciones de virus - Antivirus instalado - Error ejecutando servicios
Proactiva	Configuración de Protección contra amenazas de red (IPS)	Parámetros que determinan la configuración del módulo de protección contra amenazas de	- Habilitar IPS - Habilitar Generic Exploit Mitigation - Habilitar la prevención de intrusión en la red	- Habilitar IPS - Habilitar Generic Exploit Mitigation - Habilitar la prevención de intrusión en la red	- Habilitar IPS - Habilitar Generic Exploit Mitigation - Habilitar la prevención de intrusión en la red

Tipología	Nombre	Descripción	Reducida	Estándar	Avanzada
		red (IPS).	- Habilitar browser intrusión prevention for Windows	- Habilitar browser intrusión prevention for Windows	- Habilitar browser intrusión prevention for Windows
Proactiva	Configuración de Firewall de Antivirus	Parámetros que determinan la configuración del módulo de Firewall del cliente de antivirus.	- Habilitar FW.(es necesario definir la política por defecto y hacerla converger con las políticas y reglas definidas en los FW del centro)	- Habilitar FW.(es necesario definir la política por defecto y hacerla converger con las políticas y reglas definidas en los FW del centro)	- Habilitar FW.(es necesario definir la política por defecto y hacerla converger con las políticas y reglas definidas en los FW del centro)
Proactiva	Control de aplicaciones y dispositivos	Parámetros que determinan la configuración de los permisos a aplicaciones y dispositivos.	- Habilitar bloqueo de Autorun.inf - Deshabilitar puertos USB de usuario	- Habilitar bloqueo de Autorun.inf - Deshabilitar puertos USB de usuario	- Habilitar bloqueo de Autorun.inf - Deshabilitar puertos USB de usuario

Tabla 12: Políticas de seguridad Endpoint

13. Bibliografía

- AV-Comparatives, Malware Protection Test, https://www.av-comparatives.org/wp-content/uploads/2017/10/avc_mpt_201709_en.pdf (septiembre, 2017)
- AV-Comparatives, Support-Test, http://www.av-comparatives.org/wp-content/uploads/2016/04/avc_english_supp_2016_en.pdf (abril, 2016)
- Centro Criptológico Nacional, Esquema Nacional de Seguridad Gestión de Ciberincidentes, (julio, 2016)
- Gartner, Magic Cuadrant for Endpoint Protection Platforms, https://www.gartner.com/document/3588017?ref=solrAll&refval=195135369&qid=ae12af2cf2ff7182d4f79b7b300d9068 (enero, 2017)
- ICT Security in Enterprise, Eurostat Statistics Explained, http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises (dec, 2015)
- INCIBE (Instituto Nacional de Ciber Seguridad), Nota informativa sobre los ciberataques a varias compañías, https://www.incibe.es/sala-prensa/notas-prensa/nota-informativa-los-ciberataques-varias-companias (mayo, 2017)
- Symantec, Actualización de definiciones de virus, https://support.symantec.com/es_ES/article.TECH103326.html (2016)
- Symantec, Configuración seguridad SEPM Symantec https://support.symantec.com/es_ES/article.TECH173752.html (2017)
- Symantec, Guía de administración e instalación de Symantec Endpoint Protection 14, (Nov, 2016)
- Symantec, Product Catalog, https://www.symantec.com/products/products-az (2017)
- Symantec, Metodo de distribución de contenido, https://support.symantec.com/es_ES/article.HOWTO80888.html (2017)

- Symantec, Symantec Endpoint Protection Sizing and Scalability Best Practices (diciembre, 2016)

• Referencias

- AV-Comparatives https://www.av-comparatives.org/
- Gartner https://www.gartner.com
- MRG Effitas https://www.mrg-effitas.com
- Symantec https://www.symantec.com/es/es
- Fortinet, NGFW, https://www.fortinet.com/content/dam/fortinet/assets/alliances/dg-forticlient-symantec-endpoint-protection.pdf
- Instalación SEPM Symantec https://support.symantec.com/en_US/article.HOWTO124411.html