AGENTE LIGERO O SIN AGENTE

Una guía de las funciones de Kaspersky Security for Virtualization

Con la expansión generalizada de la virtualización, impera la necesidad de contar con soluciones de seguridad adecuadas. Aunque los entornos virtuales son tan susceptibles a los ciberataques como cualquier otro sistema físico, presentan características exclusivas que deben tenerse en cuenta a la hora de buscar soluciones de seguridad.

A pesar de que las soluciones estándar que no están específicamente diseñadas para entornos virtuales proporcionan cierto nivel de protección, pueden conllevar problemas como los que se citan a continuación:

1) **Consumo de recursos excesivo.** Esto se debe a la copia de las bases de datos de firmas y a que los motores antimalware están activos en cada máquina virtual (MV, por sus siglas en inglés) protegida.
2) **"Tormentas"**. Son actualizaciones simultáneas de bases de datos y procesos de análisis antimalware en varias máquinas virtuales que dan lugar a un aumento acelerado del consumo de recursos, lo que provoca la pérdida de rendimiento e incluso la denegación del servicio. Los intentos de mitigar el problema mediante la programación de estos procesos genera lo que se conoce como "ventanas de vulnerabilidad", periodos de tiempo en los que los análisis antimalware pospuestos hacen que las máquinas virtuales resulten vulnerables a los ataques.
3) **Brechas de seguridad instantáneas**. Las bases de datos de firmas no pueden actualizarse en máquinas virtuales inactivas, de modo que desde el arranque de la máquina hasta que finaliza el proceso de actualización, dicha máquina también es vulnerable a los ataques.
4) **Incompatibilidades.** Debido a que las soluciones estándar no están diseñadas para gestionar las funciones específicas de la virtualización, como la migración de máquinas virtuales o el almacenamiento no persistente, su uso puede dar lugar a inestabilidades e incluso a bloqueos del sistema.

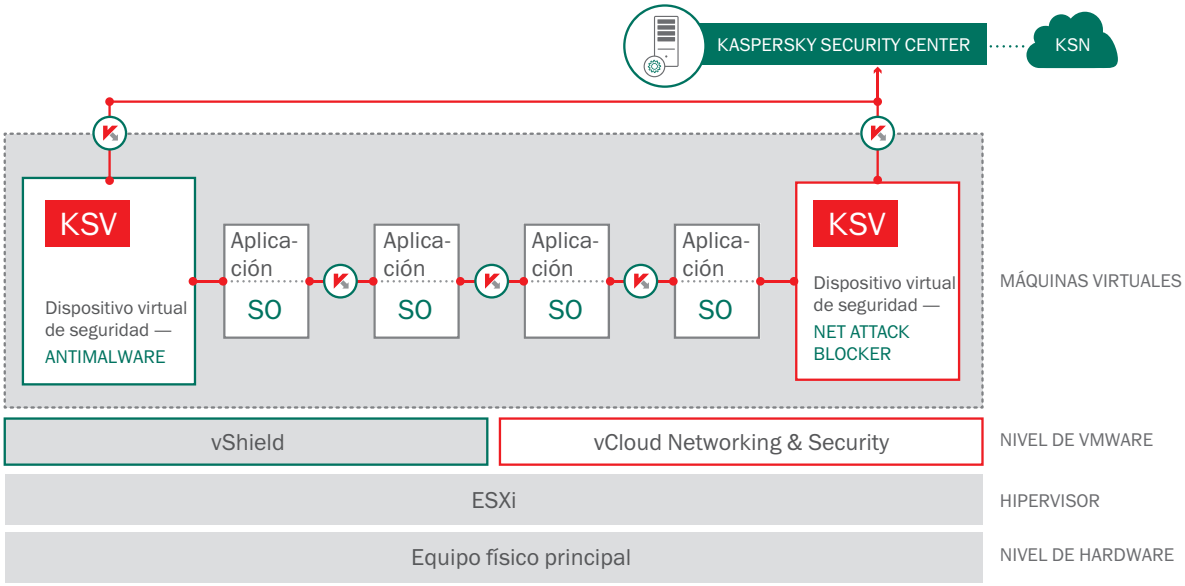
Mediante el reconocimiento de la importancia de la seguridad para sistemas virtuales, así como de las exclusivas características que presenta la virtualización, los líderes del mercado VMware han desarrollado vShield, un nivel de defensa específica para su plataforma vSphere. Este nivel crea un espacio de seguridad integrado que incorpora todos los activos virtualizados y que permite un acceso sencillo y eficiente a las soluciones de seguridad específicas. Una ventaja obvia de este enfoque es que brinda la opción de proteger "sin agentes" los endpoints virtualizados. Para eliminar la gestión de las máquinas virtuales individuales y reducir en gran medida el consumo de recursos lo único que se necesita es un dispositivo virtual de seguridad, es decir, una máquina virtual especializada que incorpora un motor de análisis antimalware y bases de datos de firmas. A través de este enfoque, las soluciones de seguridad compatibles con vShield capaces de aprovechar plenamente todas las características que ofrece el entorno de VMware pueden suponer muchas ventajas para los usuarios.

KASPERSKY SECURITY FOR VIRTUALIZATION | AGENTLESS

Kaspersky Security for Virtualization | Agentless se ha diseñado específicamente para aprovechar todas las ventajas de vShield. Presenta un dispositivo virtual de seguridad (SVA, por sus siglas en inglés), listo para su implementación inmediata, que cuenta con el galardonado motor antimalware de Kaspersky Lab y, por lo tanto, se beneficia de unos mayores índices de detección. La compatibilidad con el servicio Kaspersky Security Network con asistencia en la nube garantiza los tiempos de reacción más rápidos posibles y, lo que es más importante, reduce de manera significativa el número de falsos positivos. Además, podría utilizarse un segundo dispositivo virtual de seguridad que contara con la tecnología Network Attack Blocker de Kaspersky, junto con el componente vCloud Networking & Security de VMware.

Sin embargo, un enfoque "sin agentes" presenta sus inconvenientes.

En primer lugar, VMware es el único proveedor que ofrece un nivel de seguridad intermedio; en otras plataformas, la solución de seguridad tiene que encontrar otra forma de acceder a las máquinas virtuales individuales. En segundo lugar, vShield no proporciona acceso a los procesos internos de las máquinas virtuales, lo que disminuye de manera considerable la capacidad de cualquier solución de ofrecer una protección de mayor profundidad frente a malware avanzado en este nivel.



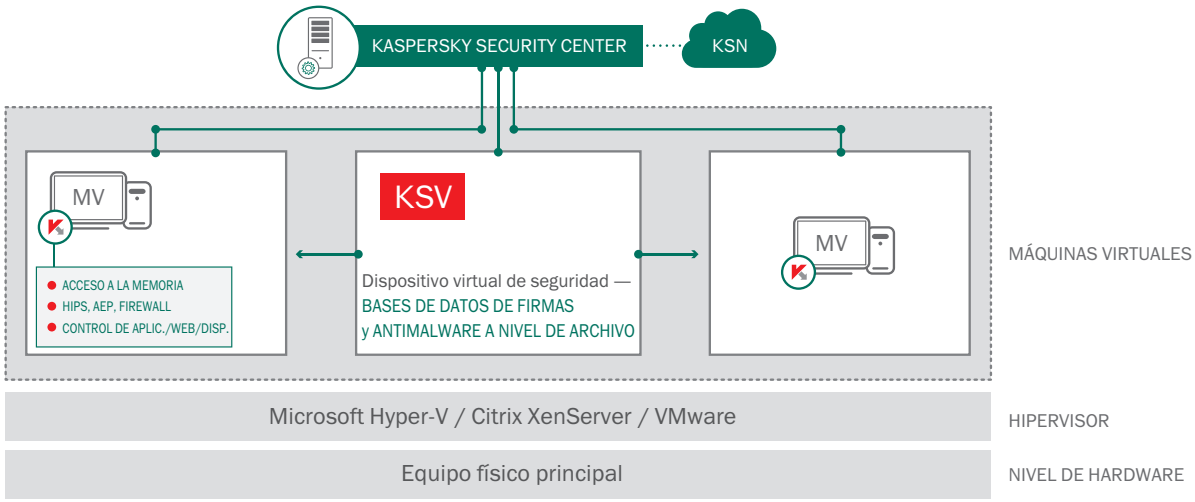
Para superar estas limitaciones, se introdujo otro enfoque: la implementación de una pequeña aplicación ligera para la máquina virtual que recibe protección, además del dispositivo virtual de seguridad. A esta aplicación se la conoce como "agente ligero". Al gestionarse de forma central el motor de análisis de archivos y las bases de datos, la aplicación tiene un impacto mucho menor en la memoria de la máquina virtual en comparación con una solución completamente basada en agentes. Además, no solo proporciona acceso al sistema de archivos de la máquina virtual, sino también a su memoria y a los procesos internos. Como resultado, se pueden emplear técnicas de seguridad más avanzadas.

KASPERSKY SECURITY FOR VIRTUALIZATION | LIGHT AGENT

Kaspersky Security for Virtualization | Light Agent se creó para las tres plataformas de virtualización más populares: Citrix, Microsoft Hyper-V y VMware. El sistema de análisis antimalware y las bases de datos de firmas residen en un exclusivo dispositivo virtual de seguridad, al igual que sucede en la tecnología sin agentes, lo que libera recursos para la implementación de otras máquinas virtuales. De este modo, se optimizan los índices de consolidación. Además, dado que hay un agente ligero que funciona dentro de cada sistema operativo invitado, a través de **Kaspersky Endpoint Security for Business** se pueden utilizar la mayoría de las avanzadas tecnologías de las que disponen los equipos físicos. De este modo, es posible implementar un conjunto completo de controles de endpoints, así como HIPS (sistemas de prevención de intrusiones basados en host), un firewall registrado y un grupo de herramientas para la gestión de sistemas. Por lo tanto, se crea un potente perímetro de defensa en varios niveles, capaz de hacer frente a los casos más sofisticados de malware e incluso a las amenazas de día cero.

Por supuesto, a pesar de que ofrece un mayor nivel de protección, la solución de agente ligero **Light Agent** puede parecer "más pesada" que su homólogo sin agentes, **Agentless**, y requiere un poco más de atención a la hora de implementar nuevas máquinas virtuales. Pero, con todo, estos inconvenientes no son tan directos como parecen.

Para comprenderlo mejor, debemos profundizar en la funcionalidad de las dos soluciones, **Agentless** y **Light Agent**, y en las amenazas que pueden contrarrestar.



AMENAZAS FRENTE A FUNCIONES

Las máquinas virtuales son tan vulnerables como las máquinas físicas, tal vez puede que incluso más. En las redes altamente virtualizadas, la propagación de infecciones puede ser devastadora. Por lo tanto, es importante identificar los puntos débiles de seguridad que presenta su infraestructura virtual para implementar las medidas adecuadas en proporción a las posibles amenazas. A continuación se analizan las posibles amenazas a las que se exponen los sistemas virtuales y las tecnologías utilizadas para combatirlas.

ARCHIVOS EJECUTABLES DE MALWARE

Es fundamental disponer de un programa antimalware para hacer frente a amenazas básicas, ya se trate de un archivos adjuntos creados con mala intención que se envían por correo electrónico, de un espacio infectado o de un archivo temporal ejecutable que contenga malware. El motor antimalware es la tecnología principal de las opciones **Agentless** y **Light Agent** de **Kaspersky Security for Virtualization**, aunque llega hasta los sistemas de archivos de la máquina virtual protegida de distintos modos en cada caso.

Otra manera de evitar que los agentes de malware dañen sus recursos virtualizados es mediante el control de aplicaciones con marcado dinámico en lista blanca. Con la ejecución de software legítimo y seguro se detiene al malware desde el primer momento. Kaspersky Security for Virtualization | Light Agent permite activar el control de aplicaciones en las máquinas virtuales, mientras que Kaspersky Security for Virtualization | Agentless, que funciona a través de vShield, no es compatible los controles de endpoints.

MALWARE "SIN CUERPO"

Algunos de los malware más sofisticados no tienen "cuerpo"; es decir, en el sistema de archivos no se encuentra nada. Este tipo de malware, que se genera a partir de un ejecutable iniciado previamente o introducido mediante un exploit, no se puede detectar con un programa antimalware convencional. En estos casos es necesario contar con avanzadas tácticas defensivas antimalware que sean capaces de supervisar los procesos que tienen lugar en la memoria y de bloquear inmediatamente los programas implicados en cualquier actividad sospechosa o peligrosa. **Kaspersky Security for Virtualization | Light Agent** está equipado con una amplia gama de tecnologías capaces de bloquear las incursiones en la memoria de la máquina virtual. Entre ellas:

- Supervisor del sistema, que controla el comportamiento de los programas y hace un seguimiento de los eventos del sistema. Esta tecnología es compatible con:
- BSS (o firmas de comportamiento en flujo), que identifican los patrones de comportamiento característicos de las actividades de malware.
- Control de privilegios, que evita que una aplicación realice cambios no solicitados, como incursiones en procesos.

Estas herramientas permiten que el sistema de protección contra intrusiones basado en host (HIPS) rastree y detenga los procesos maliciosos que tienen lugar en la memoria de la máquina virtual.

Kaspersky Security for Virtualization | Agentless solo es capaz de hacer un seguimiento de los cambios en el sistema de archivos debido a las limitaciones de la API de vShield.

EXPLOITS

La explotación de vulnerabilidades en los componentes de los sistemas y las aplicaciones más populares se encuentra entre los mecanismos de ataque más eficaces. Aunque es posible impedir estas incursiones, el programa afectado podría ejecutarse con un nivel alto de privilegios, lo que limita el control sobre sus actividades.

El método más eficaz de hacer frente a esta amenaza se basa en evitar que los exploits hagan lo que su propio nombre indica, explotar las vulnerabilidades. Esto se logra mediante el reconocimiento de la secuencia de acciones características de los exploits a medida que se desarrollan; tal y como hace la función de prevención automática contra exploits (AEP, por sus siglas en inglés) de Kaspersky. El instituto MRG Effitas fue el encargado de probar la eficacia de esta tecnología mediante una serie de pruebas independientes. Estas pruebas revelaron que, incluso con el resto de componentes de protección desactivados, la tecnología AEP de Kaspersky presentó una eficacia del 100 % frente a los ataques de exploits. Además, esta tecnología proactiva bloquea incluso los exploits de día cero desconocidos.

Kaspersky Security for Virtualization | Light Agent está equipado con esta avanzada función, lo que lo hace especialmente útil en las infraestructuras de equipos de escritorio virtualizados (VDI, por sus siglas en inglés) empleadas para sustituir a los equipos de sobremesa físicos, junto con sus respectivos riesgos de infecciones ocultas.

Kaspersky Security for Virtualization | Agentless se basa en las capacidades de vShield, que carece de funciones similares a la de la tecnología AEP de Kaspersky.

ROOTKITS

A menudo, el malware sofisticado pasa desapercibido con la ayuda de los denominados "bootkits" y "rootkits", de modo que los programas tradicionales de malware no pueden detectarlo. Estas malintencionadas herramientas cargan el malware lo más rápido posible para que pueda pasar inadvertido gracias a la obtención de privilegios altos en el sistema. La tecnología anti-rootkit de Kaspersky es capaz de detectar y erradicar incluso el malware mejor escondido. Opera en la memoria y en el sistema de archivos con el permiso de acceso a los procesos y a la memoria RAM de la máquina invitada.

Kaspersky Security for Virtualization | Light Agent puede ofrecer esta tecnología gracias a que tiene acceso completo a los recursos del equipo invitado.

Kaspersky Security for Virtualization | Agentless solo puede acceder al sistema de archivos, por lo que carece de la función anti-rootkit completa.

ATAQUES A LA RED

Existen amenazas que aprovechan las funciones del sistema de redes y permiten al atacante obtener información de vital importancia sobre la red que ataca, obtener acceso a los recursos del sistema atacado o interferir en su funcionamiento. Entre estas amenazas se incluyen el análisis de puertos, los ataques de denegación de servicio, los ataques de subdesbordamiento de búfer y otras acciones malintencionadas. Para hacer frente a dichos ataques hay que aplicar tácticas defensivas especializadas como las que proporciona la tecnología Network Attack Blocker de Kaspersky. Como su propio nombre indica, esta tecnología detiene los ataques de red entrantes con la ayuda de un sistema de detección de intrusiones (IDS, del inglés Intrusion Detection System) mediante el análisis de algoritmos heurísticos, para detectar incluso los patrones de ataque más complejos.

Tanto **Kaspersky Security for Virtualization | Agentless** como **Kaspersky Security for Virtualization | Light Agent** disponen de estas tecnologías de red entre sus funciones.

SITIOS WEB MALICIOSOS

Un sitio web malicioso o infectado es una de las fuentes de infección más comunes. Aunque casi nunca afecta a servidores virtualizados, puede plantear una grave amenaza a una infraestructura de equipos de escritorio virtualizados en caso de que los usuarios cuenten con acceso total a Internet. Aquí es donde entran en juego las tecnologías web de Kaspersky. Las soluciones antiphishing evitan que los usuarios accedan a sitios web clasificados como peligrosos a partir de la información obtenida a través de **Kaspersky Security Network** (KSN), que se actualiza continuamente con la ayuda de millones de participantes voluntarios de todo el mundo. Los sitios de phishing que aún no han sido identificados como tales también se bloquean gracias al motor heurístico que analiza el texto fuente de la página cargada y detecta signos de código malicioso. La tecnología de **control web** cuenta con la ventaja añadida de que restringe el acceso a los sitios web no relacionados con el trabajo, como sitios de juegos o redes sociales, para evitar que los usuarios pierdan tiempo en actividades ajenas a su actividad laboral.

Kaspersky Security for Virtualization | Agentless no cuenta con estas funciones basadas en host, pero sí **Kaspersky Security for Virtualization | Light Agent**, lo que hace que sea una solución más adecuada para los equipos de escritorio virtualizados con acceso a Internet.

ATAQUES BASADOS EN PERIFÉRICOS

Tradicionalmente, uno de los métodos más eficaces para introducir una infección a una red de IT ha sido mediante dispositivos de almacenamiento externo. Mientras que en la actualidad las infecciones propagadas por la red ganan importancia en términos de volumen, los dispositivos de almacenamiento externo siguen suponiendo un gran peligro, especialmente cuando forman parte de un ataque dirigido minuciosamente planificado, con un objetivo específico. Es más, los periféricos que no se utilizan para almacenar contenido también pueden suponer una amenaza importante. Entre los casos más habituales podría citarse el firmware de impresoras infectadas. Las unidades de almacenamiento externo continúan representando uno de los principales métodos para robar datos confidenciales.

Aunque no es fácil que una persona sin autorización acceda al equipo físico que aloja la infraestructura virtual, sí que es posible y hay entornos empresariales en los que esta posibilidad puede conllevar un riesgo demasiado alto. Por otro lado, en lo que respecta a los equipos de escritorio virtualizados que sustituyen equipos físicos, incluso los clientes ligeros más simples pueden tener puertos USB.

Por lo tanto, una de las precauciones que debe tomarse siempre es el control de periféricos, algo que se consigue fácilmente gracias a la tecnología de **control de dispositivos de Kaspersky**. Con esta tecnología se evita o restringe el uso de dispositivos tipos de dispositivos y bus específicos. Como es de esperar, también pueden hacerse excepciones para que aquellos periféricos esenciales para el trabajo puedan seguir usándose.

Al igual que con otras tecnologías de control o control de dispositivos, **Kaspersky Security for Virtualization | Light Agent**, ofrece la función de control de dispositivos, pero no es el caso de **Kaspersky Security for Virtualization | Agentless.**

FILTRACIÓN DE DATOS

Los secretos corporativos que se filtran de una red de IT pueden causar importantes daños a un negocio, sobre todo para la reputación de una empresa, lo que puede tener graves consecuencias a largo plazo. Por lo tanto, es necesario restringir el número de formas de compartir la información. Las funciones de **control de aplicaciones** y **control de dispositivos de Kaspersky** pueden resultar muy útiles en este caso. El control de aplicaciones puede evitar la ejecución de aplicaciones peligrosas, como los programas de mensajería instantánea o de alojamiento de archivos y aplicaciones cliente punto a punto (P2P, del inglés "peer-to-peer"). Por su parte, la función de control de dispositivos restringe el uso de dispositivos de almacenamiento externo que podrían utilizarse para robar información confidencial.

Como se ha indicado anteriormente, estas dos tecnologías están incluidas en **Kaspersky Security for Virtualization | Light Agent**, pero no en **Kaspersky Security for Virtualization | Agentless**.

AGENTLESS FRENTE A LIGHT AGENT: ¿CUÁL ES MEJOR?

A algunos lectores la respuesta puede resultarle bastante clara: **Kaspersky Security for Virtualization | Light Agent** incorpora funciones avanzadas con las que no cuenta **Kaspersky Security for Virtualization | Agentless**, de manera que la solución de "agente ligero" es, indiscutiblemente, la mejor. Pero no saquemos conclusiones precipitadas; es algo más complejo.

En primer lugar, debe tenerse en cuenta la protección instantánea que ofrece **Kaspersky Security for Virtualization | Agentless.** Las máquinas virtuales reciben protección desde el primer momento en que se inician, lo que puede suponer un problema si su red virtualizada ya tiene una infección (y su máquina virtual no puede recuperarse a partir de una imagen que contenga la aplicación **Light Agent**).

Por lo tanto, en algunos casos **Kaspersky Security for Virtualization | Light Agent** puede presentar algunos inconvenientes con respecto a **Kaspersky Security for Virtualization | Agentless** en términos de rendimiento. Para elegir la mejor opción de seguridad para su instalación virtual y sacar el máximo partido de su proyecto de virtualización, necesitará ponderar con detenimiento las posibles amenazas, el valor de los datos que desea proteger y los distintos niveles de protección necesarios.*

Tenga que cuenta que cualquier combinación de protección sin agentes para VMware y seguridad basada en agente ligero para cualquiera de las tres plataformas está cubierta por una única licencia de **Kaspersky Security for Virtualization**. Tanto si utiliza la plataforma Citrix, VMware o Microsoft, todas estarán bajo su control con la cómoda interfaz centralizada de **Kaspersky Security Center**.

* Consulte la documentación técnica sobre las diferencias de ambos productos "Kaspersky Security for Virtualization: Understand the Difference" para obtener información detallada de utilidad a la hora de elegir la mejor combinación de soluciones de Kaspersky para la protección de su infraestructura virtual.

KASPERSKY lab