

# KASPERSKY SECURITY FOR VIRTUALIZATION

*Protección superior, flexible y eficiente para servidores virtuales y VDI*

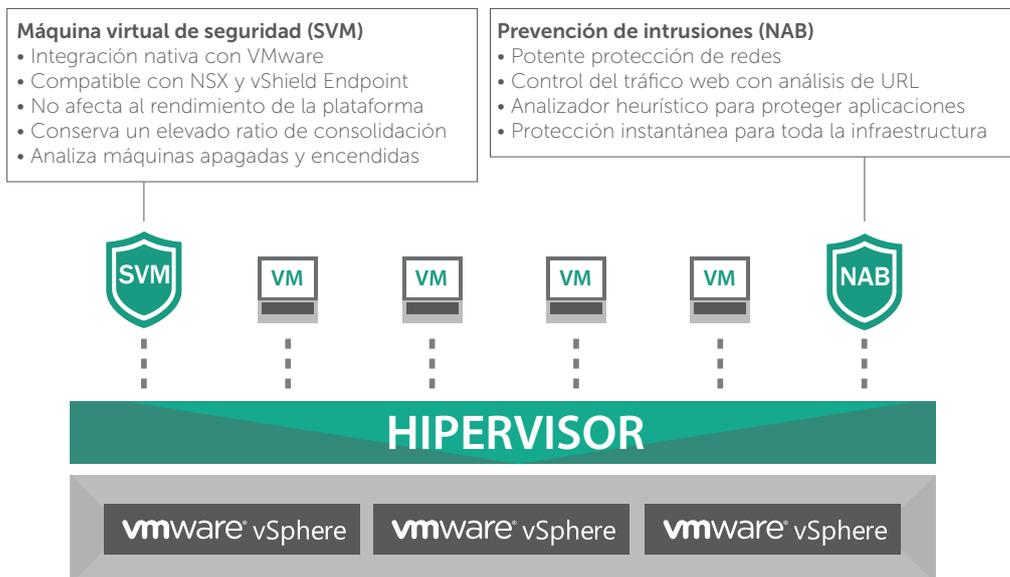
Dado el creciente número de empresas que aprovechan las ventajas de los centros de datos definidos por software, la necesidad de una protección excepcional sin comprometer la productividad nunca ha sido mayor.

Esto es exactamente lo que ofrece Kaspersky Security for Virtualization: excepcional, potente y exhaustiva protección de varios niveles para VDI, y entornos y servidores virtuales, mejorada gracias a la estrecha integración con las tecnologías y plataformas de virtualización más populares: VMware vSphere con NSX, Microsoft Hyper-V, Citrix XenServer y KVM, así como VMware Horizon y Citrix XenDesktop.

Con Kaspersky Security for Virtualization, que incorpora opciones de seguridad sin agentes y con agente ligero, redefinimos cómo interactúan su centro de datos definido por software y su solución de seguridad, potenciando ambos para que sean más inteligentes, rápidos y eficientes.

## Integración sin agentes con VMware NSX

La interacción nativa entre una plataforma de virtualización y sus soluciones de seguridad permite a su centro de datos definido por software reaccionar en tiempo real a cualquier incidente de seguridad en toda su infraestructura.



- **El motor antimalware más premiado** mejorado con IDS/IPS en la red virtual reconoce y bloquea ciberamenazas conocidas, desconocidas y de día cero.
- **Implementación completamente automatizada** de dispositivos de seguridad especializados, en función de las políticas de seguridad aplicadas a cada máquina virtual en el host de hipervisor.
- **La integración con las políticas de seguridad de NSX** permite que cada máquina virtual reciba capacidades de seguridad precisas y exhaustivas que le permitirán crear y ampliar su infraestructura sin límites.
- **La integración con las etiquetas de seguridad de NSX** permite que el centro de datos definido por software reaccione a tiempo real sobre cualquier incidente de seguridad y reconfigure automáticamente toda la infraestructura virtual si es necesario.
- **Defensa proactiva contra amenazas sofisticadas** mediante el uso de Security Network basado en la nube.

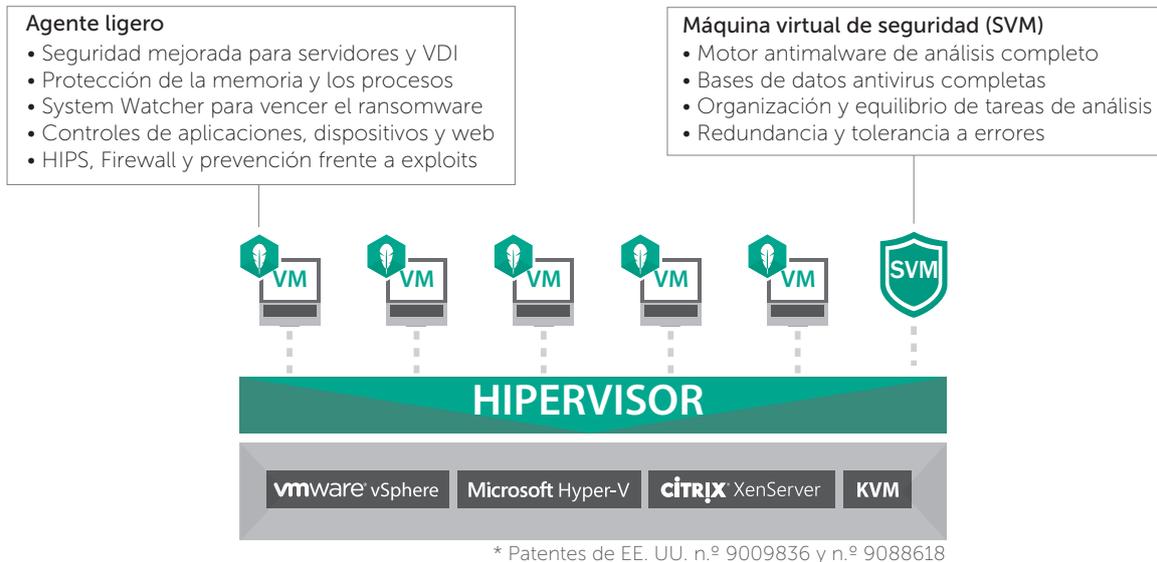


## Más niveles de seguridad con Light Agent

Aunque la integración sin agentes con VMware NSX proporciona una mayor automatización, los escritorios y servidores virtuales fundamentales para su empresa requieren mayores niveles de protección, ya que la infraestructura de red y las actividades de archivos no son los únicos vectores para ciberataques. Necesita más seguridad.

Kaspersky Security for Virtualization Light Agent brinda una solución única para proteger tanto servidores virtuales como VDI. Gracias a su compatibilidad con las plataformas más populares, entre las que se incluyen VMware vSphere, Citrix XenServer, Microsoft Hyper-V y KVM, esta solución es ideal para los centros de datos híbridos definidos por software. Un agente de seguridad potente y ligero es compatible con las plataformas VDI líderes del sector, como Citrix XenDesktop y VMware Horizon, e incrementa significativamente la protección a la vez que conserva el rendimiento de cada máquina virtual.

### FUNCIONAMIENTO Y FINALIDAD



Una máquina virtual de seguridad (SVM) en cada host analiza todas las máquinas virtuales de forma centralizada, al tiempo que un potente agente ligero implementado en cada máquina virtual ofrece funciones avanzadas de seguridad, incluidos los controles de aplicaciones, dispositivos y web, protección antimalware para el tráfico web y el correo, además de análisis heurísticos avanzados. También se reducen los picos en el consumo de recursos al organizar de forma inteligente las tareas de análisis, automatizando las colas mediante la agrupación y el establecimiento de prioridades de las tareas de análisis en varias máquinas virtuales protegidas.

- La tecnología **System Watcher** utiliza las firmas de comportamiento en flujo para preservar la coherencia de cada VDI y proteger contra bloqueadores de cifrado y ransomware.
- La **supervisión del inicio de aplicaciones y privilegios**, incluida la denegación predeterminada, permite controlar la actividad del usuario para que solo se inicien aplicaciones de confianza en una máquina virtual protegida.
- **Network Attack Blocker con un moderno sistema de prevención de intrusiones basado en host** protege el entorno virtualizado contra ataques basados en red.
- La **protección URL** protege cada máquina virtual contra el malware y los recursos maliciosos de Internet que puedan dañar o no cumplan las políticas de seguridad corporativas.
- La **protección del tráfico web y del correo electrónico** garantizan que todas las comunicaciones dentro de su entorno corporativo sean seguras y no contengan malware.
- El **control de dispositivos** garantiza acceso seguro a los dispositivos virtualizados que están conectados a un escritorio virtual.

Sea cual sea la plataforma o plataformas virtualizadas que utilice, Kaspersky Security for Virtualization, con sus tecnologías perfectamente diseñadas y una arquitectura única proporciona mayores capacidades de seguridad. Se trata de una única solución de seguridad compatible con VMware vSphere con NSX, Microsoft Hyper-V, Citrix XenServer y KVM. Con independencia de la configuración e hibridación de su plataforma, dentro o fuera de las instalaciones, toda la gestión de la seguridad se efectúa a través de una consola unificada y se conserva la eficiencia de los sistemas.

Kaspersky Security for Virtualization Light Agent y Agentless. Dos enfoques de seguridad en una única solución, que proporciona una potente protección combinada con rendimiento eficiente para su entorno virtual.

Para obtener más información acerca de Kaspersky Security for Virtualization, visite [www.kaspersky.com/enterprise](http://www.kaspersky.com/enterprise)