



# Protección de entornos virtualizados

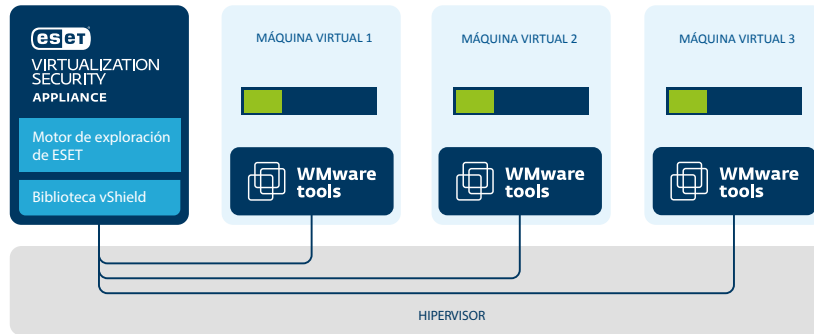


ENJOY SAFER TECHNOLOGY™



# eset VIRTUALIZATION SECURITY FOR VMWARE VSHIELD

El appliance virtual de ESET Virtualization Security provee protección sin agente a todas las máquinas virtuales que se encuentren en el hosts que tengan instalado el ESET Virtualization Security, ya que se conecta automáticamente con el appliance vShield.



Además, la solución soporta VMware vMotion y vCenter en forma nativa, y también es compatible con ESET Remote Administrator 6, la consola de ESET basada en la Web. La consola ofrece una visión general y a la vez permite desglosar cada máquina virtual para ejecutar tareas con suma rapidez, logrando una gestión completa de la seguridad en todos los endpoints.

## Fácil de desplegar

El reemplazo de todos los appliance virtuales es tan simple como registrar un nuevo SVA (dispositivo virtual de seguridad) en vShield Manager. Cuando se instala ESET Remote Administrator (que también se suministra como appliance virtual) se pueden desplegar los appliance de ESET Virtualization Security en múltiples hosts al mismo tiempo.

## Rendimiento superior

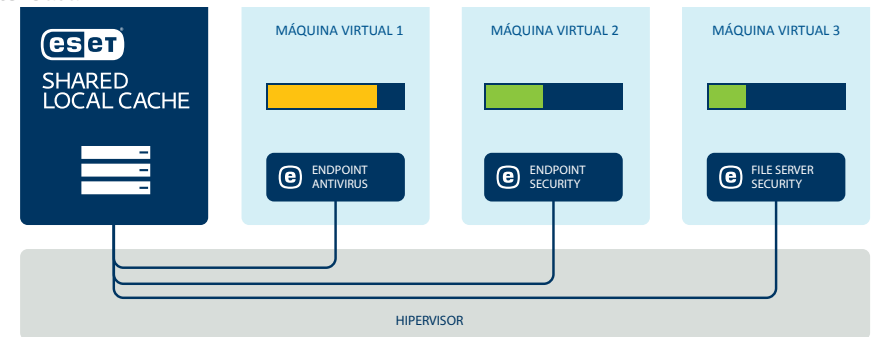
La infraestructura de las máquinas virtuales requiere que se optimicen los recursos y el rendimiento; y el motor de exploración de ESET cumple exactamente con estos requisitos. Es reconocido por su baja demanda de recursos del sistema y su alta velocidad, por lo que deja más recursos disponibles para otras aplicaciones y procesos.

## Evita las tormentas antivirus

Todas las tareas en acceso y bajo demanda se descargan a través de las herramientas VMware hasta un módulo de exploración centralizado ubicado dentro del appliance de ESET Virtualization Security, lo que previene efectivamente las tormentas antivirus y los problemas de rendimiento.

# eset SHARED LOCAL CACHE

Con la Caché local compartida de ESET y la protección de uno de los productos de seguridad de ESET basado en agentes, obtendrá el mismo conjunto de herramientas y funcionalidades de seguridad que en un entorno físico, además de una velocidad de exploración sumamente potenciada.



**Endpoint Antivirus:** ESET Endpoint Antivirus 6 para Windows, ESET Endpoint Antivirus 6 para OS X

**Endpoint Security:** ESET Endpoint Security 6 para Windows, ESET Endpoint Security 6 para OS X

**File Server Security:** ESET File Security 6 para Microsoft Windows Server

**Mail Server Security:** ESET Mail Security 6 para Microsoft Exchange Server

## Evita las exploraciones duplicadas

Las máquinas virtuales suelen compartir la misma imagen de base, es decir que entre 70% y 80% de sus archivos son duplicados. La Caché local compartida de ESET guarda los metadatos sobre los archivos no infectados de las máquinas ya exploradas dentro del mismo hipervisor. Esto significa que los archivos ya explorados en una máquina virtual no se vuelven a explorar en forma reiterada en otras máquinas virtuales que tengan el mismo entorno virtual, lo que genera un incremento significativo de la velocidad.

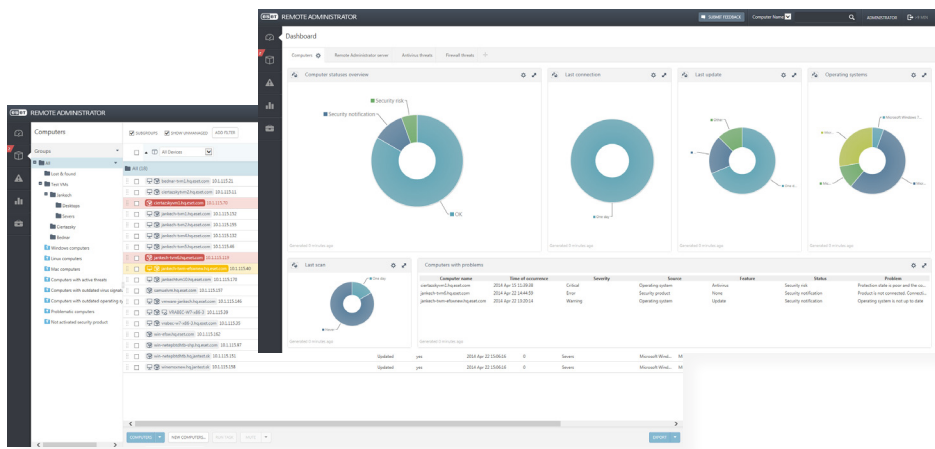
## Protección en varias capas

La Caché local compartida de ESET, combinada con una solución de ESET basada en agentes, le proporciona seguridad integral de TI para su empresa mediante múltiples capas de protección, entre las que se incluyen nuestra comprobada tecnología de detección ESET NOD32® y opciones de exploración completamente personalizables.

Las máquinas físicas y virtuales se administran desde un mismo lugar, de modo que se puede usar la administración basada en roles. Además, el panel de control basado en la Web suministra información general completa a simple vista, a la vez que permite desglosar la información para ejecutar cualquier acción que se considere necesaria.

Asimismo, ESET Remote Administrator puede instalarse en servidores Windows y Linux, y también se ofrece como un appliance virtual.

El appliance virtual de ESET Remote Administrator simplifica su despliegue y es mucho más veloz que si se usa el instalador integrado o los paquetes de instalación de los componentes.



Soporta hipervisores nativos/sin sistema operativo (VMware vSphere/ESXi, Microsoft Hyper-V), así como hipervisores que suelen funcionar con sistemas operativos para equipos de escritorio (VMware Workstation, VMware Player, Oracle VirtualBox).

El appliance virtual se suministra como un archivo OVA (Open Virtualization Appliance) y contiene varios tipos de dispositivos ESET Remote Administrator (un componente para servidor que incluye un detector de equipos no autorizados, un componente para proxy y un componente para la administración de dispositivos móviles).

## Exclusiones de procesos

El administrador puede definir los procesos que el módulo de protección en tiempo real debe ignorar; todas las operaciones con archivos que se atribuyan a estos procesos excluidos se considerarán seguros. Esto es útil en particular para actividades que suelen interferir con la protección en tiempo real, como la creación de backups o la migración en vivo de máquinas virtuales. Sin embargo, hay que tener en cuenta que los procesos excluidos pueden acceder a archivos u objetos no seguros sin accionar ninguna alerta de seguridad.

## Independencia de instantáneas

Las actualizaciones y los módulos del programa de ESET se pueden almacenar fuera de la ubicación predeterminada, es decir que no se ven afectados cuando una máquina virtual revierte su configuración a una instantánea anterior. En consecuencia, no es necesario descargar las actualizaciones y los módulos cada vez que se revierte la máquina virtual a una instantánea anterior. Además, la máquina que revirtió su instantánea puede utilizar las actualizaciones intactas y evitar grandes descargas, lo que acelera el tiempo de recuperación de la instantánea.

## Soporte nativo para entornos de clúster

Le permite configurar la solución para que replique automáticamente la configuración cuando se instala en un entorno de clústers y permite administrarlos como si fueran uno solo, eliminando la necesidad de replicar manualmente los cambios de configuración en otros nodos del clúster.

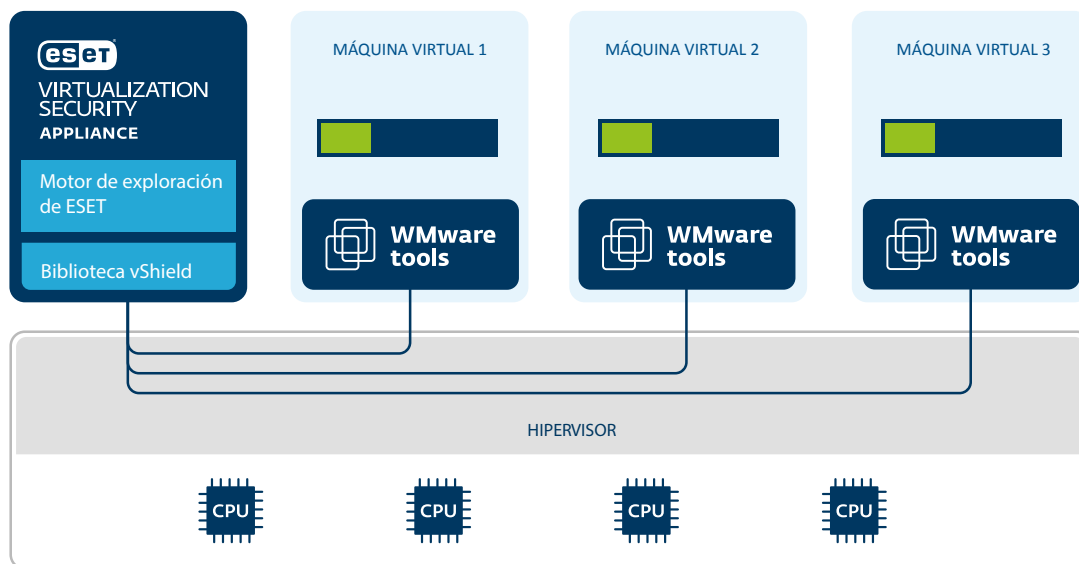
## Exploración del almacenamiento en Hyper-V

Explora los servidores de Microsoft Windows® con el rol Hyper-V en busca de malware, sin necesidad de instalar ninguna otra instancia del producto antivirus. Ahorra tiempo, ya que explora el contenido del disco rígido sin arreglos previos ni períodos de inactividad, y proporciona informes separados según los resultados de la exploración. Para mejorar el rendimiento de los sistemas y reducir el consumo de memoria de la CPU, se pueden configurar las exploraciones de las máquinas virtuales para que se lleven a cabo mientras están apagadas.

Si desea conocer las características disponibles para cada producto, visite [eset-la.com](http://eset-la.com).

## Licenciamiento de ESET Virtualization Security para VMware vShield

Elija entre 3 tipos de licencias diferentes: por máquina virtual, por host o por procesador, según lo que mejor se adapte a sus necesidades, la infraestructura de la red y el modo en que usa su entorno virtual



### Licenciamiento por máquina virtual (VM)

- 1 VM se cuenta como 1 endpoint física y consume un lugar de la licencia
- Es la solución ideal si se ejecutan menos de 50 VM en el host
- Es la solución más apropiada para empresas que se encuentran en el proceso de migración de entornos físicos a virtuales: la licencia de ESET se migra de endpoints físicas a virtuales

### Licenciamiento por host

- Tarifa plana: un host = un precio
- Cubre una cantidad ilimitada de VM ejecutándose en el host
- Es la solución más apropiada si se ejecutan más de 50 VM en el host

### Licenciamiento por procesador

- Tarifa plana: un procesador físico = un precio
- Precio por 2 procesadores = aproximadamente el precio para 1 host
- Es la solución más apropiada si se ejecutan más de 25 VM por procesador

## Licenciamiento de la Caché local compartida de ESET

La Caché local compartida de ESET se suministra sin cargo con la compra de cualquier producto de seguridad de ESET (es necesario que al menos uno de ellos esté presente en cada máquina virtual).