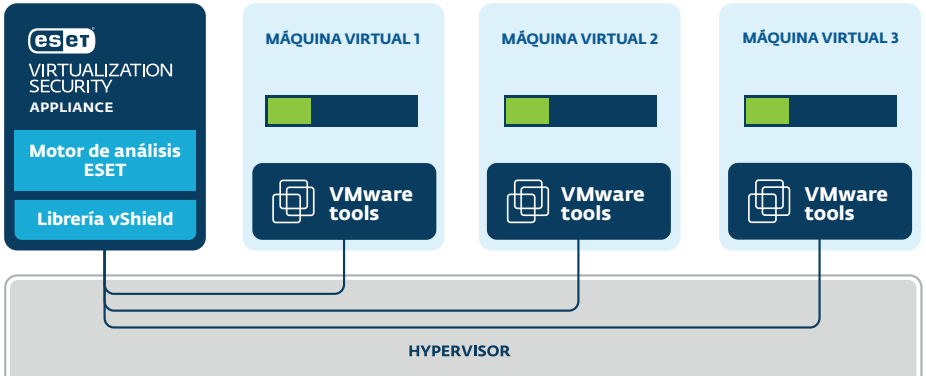
Protegiendo entornos virtualizados

vmware READY
NETWORKING Y SEGURIDAD

ENJOY SAFER TECHNOLOGY™

VIRTUALIZATION SECURITY
PARA VMWARE VSHIELD

El "appliance" de ESET Virtualization Security reestructura la protección sin agente de todas las máquinas virtuales de cada host en el que está instalada, conectando automáticamente con la "appliance" de vShield.



Además, el producto es compatible con VMware vMotion y vCenter, y también con ESET Remote Administrator 6, la consola web de ESET, permitiéndote un gran nivel de control para máquinas virtuales para una rápida ejecución de tareas y una administración completa de la seguridad del equipo.

Fácil de instalar

Sustituir cada "appliance" virtual es tan simple como registrar una nueva "appliance" virtual de seguridad (SVA) dentro del administrador vShield. Una vez instalado ESET Remote Administrator, que también está disponible como "appliance" virtual, pueden instalarse las "appliances" de ESET Virtualization Security en múltiples servidores a la vez.

Alto rendimiento

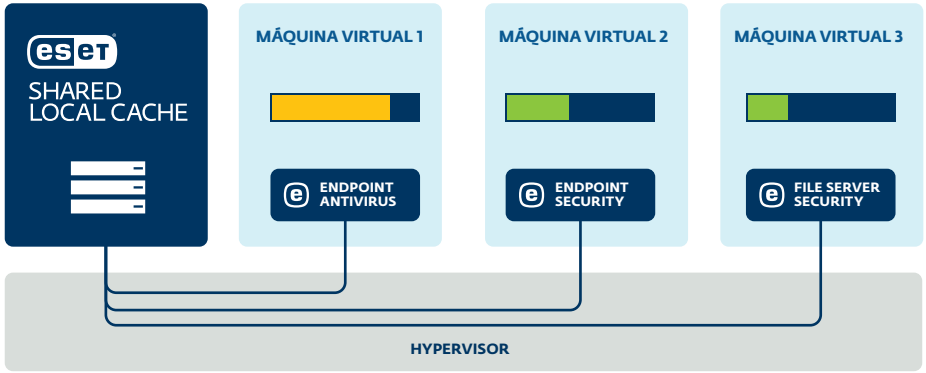
La infraestructura de máquinas virtuales trata de optimizar los recursos y el rendimiento, y el motor de análisis de ESET cumple exactamente estos requisitos. Es muy conocido por su bajo consumo de recursos y alta velocidad, dejando libres más recursos del sistema para otras aplicaciones y procesos.

Cero inconvenientes

Todas las tareas de análisis inicial y bajo demanda son transferidas mediante VMware tools a un analizador centralizado dentro de la aplicación ESET Virtualization Security, evitando eficazmente los posibles inconvenientes del agente antivirus e incidencias relacionadas con el rendimiento.

SHARED LOCAL CACHE

Con ESET Shared Local Cache y la protección de un producto de seguridad ESET basado en agente, consigues las mismas herramientas y características de seguridad que tendrías en un entorno físico, además de un incremento en la velocidad de análisis.



Endpoint Antivirus: ESET NOD32 Endpoint Antivirus 6 para Windows, ESET NOD32 Endpoint Antivirus 6 para OS X.

Endpoint Security: ESET NOD32 Endpoint Security 6 para Windows, ESET NOD32 Endpoint Security 6 para OS X.

Seguridad para servidor de archivos: ESET NDO32 File Security 6 para Microsoft Windows Server.

Seguridad para servidor de correo: ESET NOD32 Mail Security 6 para Microsoft Exchange Server.

Sin duplicación de análisis

Las máquinas virtuales comparten normalmente la misma imagen de base, con lo que se duplica un 70-80% de archivos entre máquinas. ESET Shared Local Cache almacena metadatos de archivos limpios de las máquinas analizadas anteriormente dentro del mismo hipervisor. Esto significa que los archivos ya analizados en una máquina virtual no se analizan de nuevo en otra máquina virtual dentro del mismo entorno virtual, aumentando significativamente la velocidad del análisis.

Protección multicapa

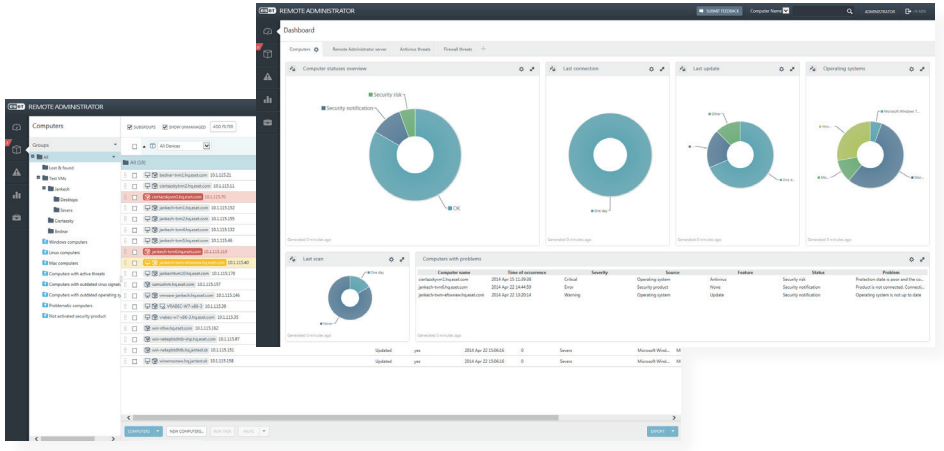
ESET Shared Local Cache, en combinación con un producto ESET basado en agente, proporciona una seguridad informática completa para tu empresa mediante múltiples capas de protección, que incluyen nuestra tecnología de detección ESET NOD32® y muchas opciones para personalizar el análisis.

REMOTE ADMINISTRATOR

Las máquinas físicas y virtuales se administran desde un único punto mediante ESET Remote Administrator, permitiendo una administración basada en perfiles y un panel de administración web muy intuitivo con amplias posibilidades de personalización que pueden utilizarse para ejecutar cualquier acción necesaria.

ESET Remote Administrator puede instalarse en servidores Windows y Linux, y también como "virtual appliance".

La "virtual appliance" de ESET Remote Administrator simplifica su instalación y es más rápido de implementar que utilizando el instalador todo en uno o la instalación por componentes.



Es compatible con hipervisores nativos/bare-metal (VMware vSphere/ESXi, Microsoft Hyper-V) así como con hipervisores en el servidor que funcionan normalmente en sistemas operativos de Escritorio (VMware Workstation, VMware Player, Oracle VirtualBox).

La "virtual appliance" viene como archivo OVA (Aplicación de virtualización abierta) y es compatible con la mayoría de entornos virtuales. Incluye además el "rogue detector sensor", el componente proxy y el componente para administración de dispositivos móviles.

SERVER SOLUTIONS
LISTO PARA ENTORNOS VIRTUALES

Exclusión de procesos

El administrador puede definir procesos que son ignorados por el módulo de protección en tiempo real. Todas las operaciones de archivos que se pueden atribuir a estos procesos con privilegios se consideran seguras. Esto es útil para procesos que interfieren a menudo con la protección en tiempo real, como la copia de seguridad o la migración a máquinas virtuales. El proceso excluido puede acceder incluso a archivos no seguros o a objetos sin lanzar una alerta.

Independiente de snapshots

Las actualizaciones de ESET y los módulos del programa se pueden almacenar fuera de la ubicación predeterminada, para que no se vean afectados al revertir a un punto previo de restauración (snapshot) de la máquina virtual. Como resultado, las actualizaciones y módulos no tienen que descargarse cada vez que una máquina virtual vuelve a un punto previo de restauración y la máquina revertida puede utilizar actualizaciones intactas y evitar grandes descargas, obteniendo un menor tiempo de recuperación.

Soporte para clústers

Te permite configurar el producto para que replique automáticamente la configuración cuando se instala en un entorno de clúster y administrarlo como uno solo, eliminando así la necesidad de replicar los cambios en la configuración de forma manual a otros nodos del clúster.

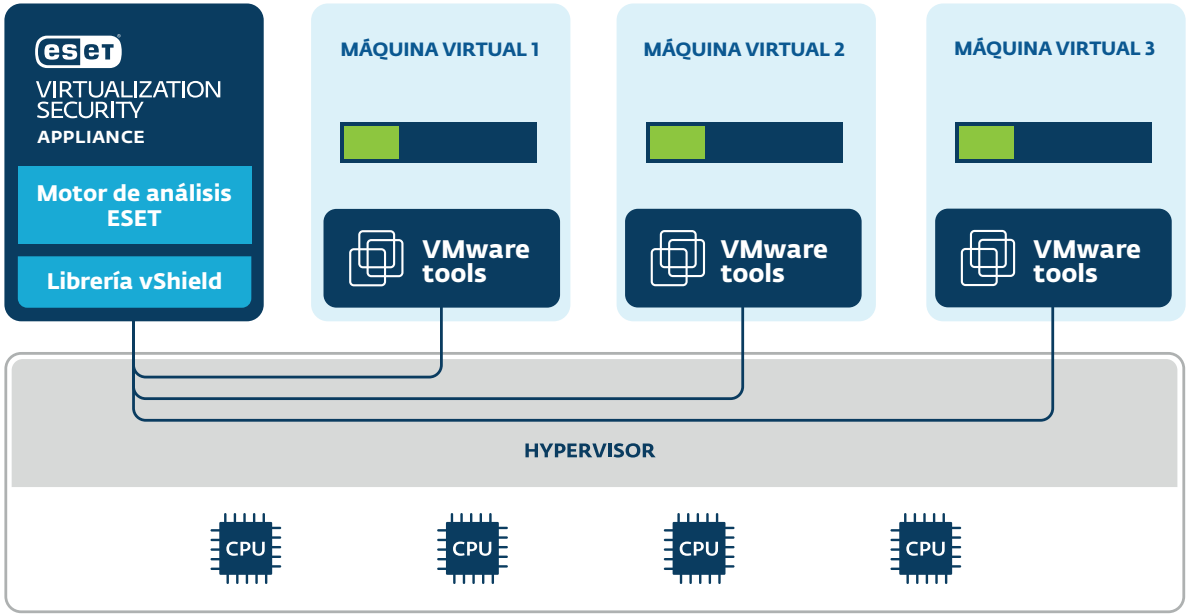
Análisis de almacenamiento en Hyper-V

Analiza los servidores Microsoft Windows® con rol de Hyper-V habilitado en busca de amenazas, sin necesidad de tener instalado un producto antivirus. Ahorra tiempo al analizar el contenido de los discos duros, sin necesidad de realizar tareas previas ni pausas, y crea informes separados según los resultados del análisis. Para un mejor rendimiento, un menor consumo de memoria y uso de la CPU, los análisis pueden llevarse a cabo en máquinas virtuales mientras están apagadas.

Para ver qué características son aplicables a qué productos, por favor visita **eset.es**.

Licenciamiento de ESET Virtualization Security para VMware vShield

Puedes elegir tres tipos diferentes de licenciamiento: por máquina virtual, por host o por procesador; de forma que se adapte a tus necesidades, a la infraestructura de red y a la forma en la que usas tu entorno virtual.



Licenciamiento por máquina virtual (MV)

- 1 MV cuenta como un equipo físico y consume un puesto de la licencia
- Es la solución ideal si tienes menos de 50 MV en el host
- Es la solución más apropiada para empresas en proceso de migración de entornos físicos a virtuales. Migra la licencia ESET de equipos físicos a virtuales

Licenciamiento por servidor

- Tarifa plana: un servidor = un precio
- Número ilimitado de MV instaladas en el servidor protegido
- Es el más apropiado si se instalan más de 50 MV en el servidor

Licenciamiento por procesador

- Tarifa plana: un procesador físico = un precio.
- Precio para 2 procesadores = aproximadamente el precio para 1 servidor
- Es la opción más apropiada si se montan más de 25 MV por procesador

Licenciamiento de ESET Shared Local Cache

ESET Shared Local Cache es gratis con la licencia de cualquier producto de seguridad ESET para empresas. Al menos uno de ellos debe estar presente en cada máquina virtual.