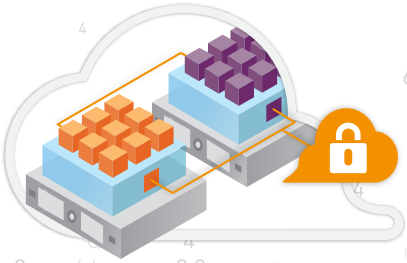
SafeNet | THE DATA PROTECTION COMPANY



ProtectV™

Protección de datos para la nube

INFORME DEL PRODUCTO

Los riesgos de seguridad de la virtualización

Las diferencias estructurales entre los entornos físicos y virtuales pueden comprometer la integridad de los datos, reducir el control sobre el acceso de los usuarios, comprometer el cumplimiento y aumentar la responsabilidad.

Amplia distribución de VMs

- Se replican fácilmente mediante sencillos snapshots
- Están respaldadas en los distintos centros de datos de todo el mundo
- Los snapshots y copias de seguridad son fáciles de mover, copiar o robar sin ser detectadas

Usuarios más privilegiados

- Los administradores y usuarios con privilegios a menudo operan de forma independiente
- Datos de circulación conjunta en entornos de múltiples clientes
- Es difícil garantizar la separación de tareas entre el proveedor de servicios en la nube y los superusuarios de la organización

La nube proporciona la agilidad, elasticidad, capacidad y redundancia necesarias para mantener una ventaja competitiva en el mercado. A medida que las empresas pasan sus servidores de centros de datos físicos específicos a infraestructuras virtuales o a nubes públicas de múltiples clientes, híbridas o privadas, disfrutan de ventajas sustanciales en costes y eficiencia.

Sin embargo, este traspaso añade un nivel adicional de retos de seguridad específicos de la virtualización. Las organizaciones cada vez se enfrentan a más retos para garantizar una potente seguridad de la información. Incluso en nubes privadas y entornos más aislados como los centros de datos virtuales, los datos todavía están en riesgo de quedar expuestos.

Presentamos ProtectV de SafeNet, la primera solución del sector de alta seguridad y exhaustiva para proteger tanto la infraestructura virtual como los datos, lo cual proporciona a las organizaciones la libertad para migrar a entornos virtuales y en la nube a la vez que mantienen la propiedad, el cumplimiento y el control total de los datos.

Proteja sus datos en entornos virtuales y en la nube con ProtectV

Ventajas empresariales	Funciones
La primera "caja de seguridad" de confianza para la protección de entornos virtuales El cifrado completo de tanto VMs como volúmenes de almacenamiento combinados con la autenticación pre-arranque "a prueba de manipulaciones", garantiza el aislamiento total de los datos y la separación de las tareas. ProtectV hace que las máquinas virtuales y los volúmenes de almacenamiento sean tan seguros como los servidores físicos en el entorno de almacenamiento más robusto y seguro en instalaciones locales. ProtectV permite que las empresas controlen la recuperación de datos y la destrucción digital, dejando las copias ilegítimas y los snapshots o copias ocultas inutilizadas.	**Cifrado completo de almacenamiento y máquinas virtuales:** • Permite el cifrado de todas las máquinas virtuales y los volúmenes de almacenamiento asociados a ellas • No se escriben datos en la partición del sistema o en el volumen de disco sin cifrarse previamente • Quedan protegidos incluso los datos almacenados en una partición del sistema operativo. • Las claves de cifrado se almacenan en instalaciones locales, en un gestor de claves basado en HW de alta seguridad.
La única solución de alta seguridad para el cumplimiento de datos La gestión de claves basada en hardware en instalaciones locales junto con la autenticación pre-arranque y el control de acceso granular proporcionan un dominio indiscutible y una prueba de propiedad de los datos y las claves. ProtectV protege los datos virtualizados, lo cual evita la exposición no autorizada de los datos o el abuso de los superusuarios y ayuda a cumplir con toda una serie de normativas como PCI y HIPAA.	**Autenticación pre-arranque:** • El acceso a datos almacenados o procesados por una máquina virtual protegida requiere la autenticación del usuario y la autorización explícita por parte de ProtectV. **Separación de tareas:** • Las normativas de cifrado basadas en funciones, junto con la gestión de claves segregada garantizan la separación de tareas entre los administradores de los sistemas del proveedor de servicios en la nube y los administradores de TI de la organización, o entre las distintas unidades del propio entorno virtual de la organización.
Visibilidad y prueba de gobernanza de datos SafeNet refuerza el control con un nivel robusto de seguridad y proporciona el cumplimiento de normativas y un punto de auditoría centralizado y único que permite que la gobernanza de los datos recaiga en la autorización explícita y el registro de cada evento de acceso en las VMs protegidas.	**Gestión de la seguridad en los entornos en la nube:** • Una plataforma de gestión unificada sirve como punto de auditoría central proporcionando una vista de panel general de todas las máquinas virtuales cifradas y sin cifrar y de los volúmenes de almacenamiento que pertenecen a la organización. **Gestión del ciclo de vida de las claves empresariales con seguridad de nivel gubernamental:** • La única solución que proporciona una gestión de claves en las instalaciones con la alta seguridad de dispositivos KeySecure con certificación de nivel 3 FIPS 140-2.

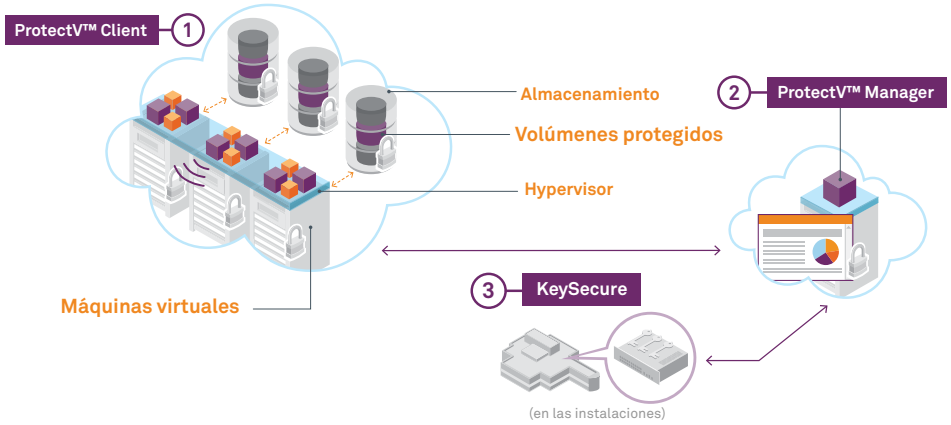
1. Instale ProtectV Client en sus VMs. Seleccione qué servidores y qué volúmenes de almacenamiento desea cifrar y cree sus normativas.

2. ProtectV Manager es una máquina virtual que funciona como una AWS AMI o como una VM en un entorno VMware. Configure ProtectV Manager mediante la creación de usuarios y permisos.

3. Keysecure es el componente que ofrece el mayor nivel de seguridad. Instale KeySecure en las instalaciones como su fuente de confianza para la gestión del ciclo de vida de todos los tipos de clave de sus centros de datos y nubes públicas y privadas.

ProtectV: Cómo funciona

ProtectV protege los datos regulados en las VMs y los volúmenes de almacenamiento en centros de datos virtuales y nubes públicas y privadas.

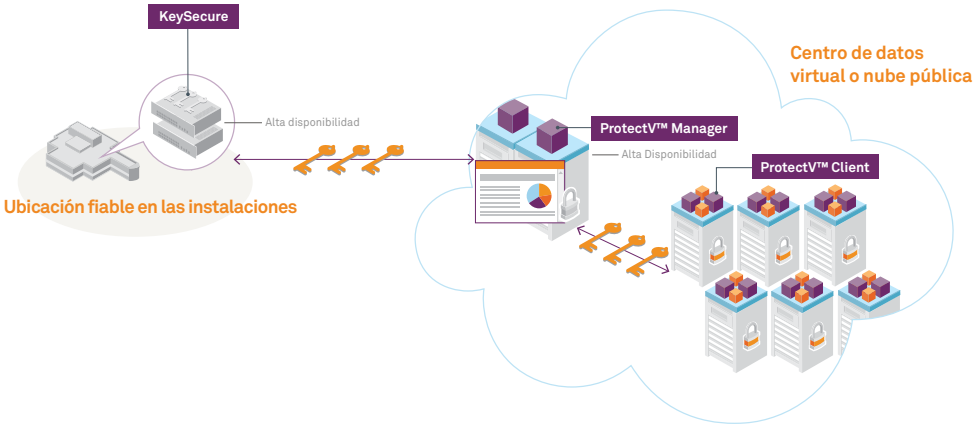


Escenarios de despliegue

Tanto si los datos se almacenan en un entorno virtual como VMware vCenter o en una nube pública o privada como Amazon Web Services EC2/EBS o Amazon VPC, ProtectV Manager puede desplegarse fácilmente utilizando imágenes predefinidas. ProtectV está equipado con un GUI fácil de utilizar para gestionar las normativas, usuarios y funciones y realizar la supervisión del sistema y la gestión de eventos.

Además, ofrece APIs para la automatización e integración con sistemas de aprovisionamiento de servidor virtual y CLIs para los scritps y operaciones en lotes y así obtener una mejor agilidad y un aprovisionamiento rápido.

Escenarios de despliegue de ProtectV para centros de datos virtuales y nubes públicas y privadas



Especificaciones técnicas

Plataformas compatibles

- Amazon Web Services EC2
- Amazon VPC
- VMware vCenter

Sistemas operativos compatibles

- Microsoft Windows Server 2008 32-bit
- Microsoft Windows Server 2008 R2 64-bit
- Microsoft Windows Server 2003 R2 64-bit
- CentOS Linux 5.5 64-bit
- CentOS Linux 5.6 64-bit
- CentOS Linux 5.6 32-bit
- Red Hat Enterprise Linux (RHEL) 5.6 32- y 64-bit

Navegadores compatibles con ProtectV Manager

- Internet Explorer 8, 9
- Firefox 4.0.1, 5.0, 6.0
- Google Chrome 12.0 y posterior

Productos de gestión de claves empresariales de SafeNet compatibles

- SafeNet KeySecure k460
- SafeNet KeySecure k150
- SafeNet DataSecure i450
- SafeNet DataSecure i150

Protección de datos de SafeNet

Las soluciones de seguridad en entornos virtualizados y en la nube, como toda seguridad empresarial, tienen que ser gestionadas con una visión por capas del ciclo de vida de la protección de la información que combine el cifrado, las normativas de acceso, la gestión de claves, la seguridad de contenidos y la autenticación. Estos niveles deben estar integrados en un marco flexible que permita a las empresas adaptarse a los riesgos a los que se enfrentan. Donde quiera que residan los datos, SafeNet ofrece un almacenamiento persistente y seguro para los datos con y sin estructura. SafeNet proporciona un marco práctico para la provisión de la confianza, seguridad y cumplimiento que exigen las empresas cuando mueven datos, aplicaciones y sistemas a entornos virtuales y en la nube.

Contacto: Para consultar todas las localizaciones de ofi cinas e información de contacto, visite **www.safenet-inc.com**
Síganos: www.safenet-inc.com/connected