Ransomware:

Crear un **backup** seguro como su última línea de **defensa**

Dave Russell,

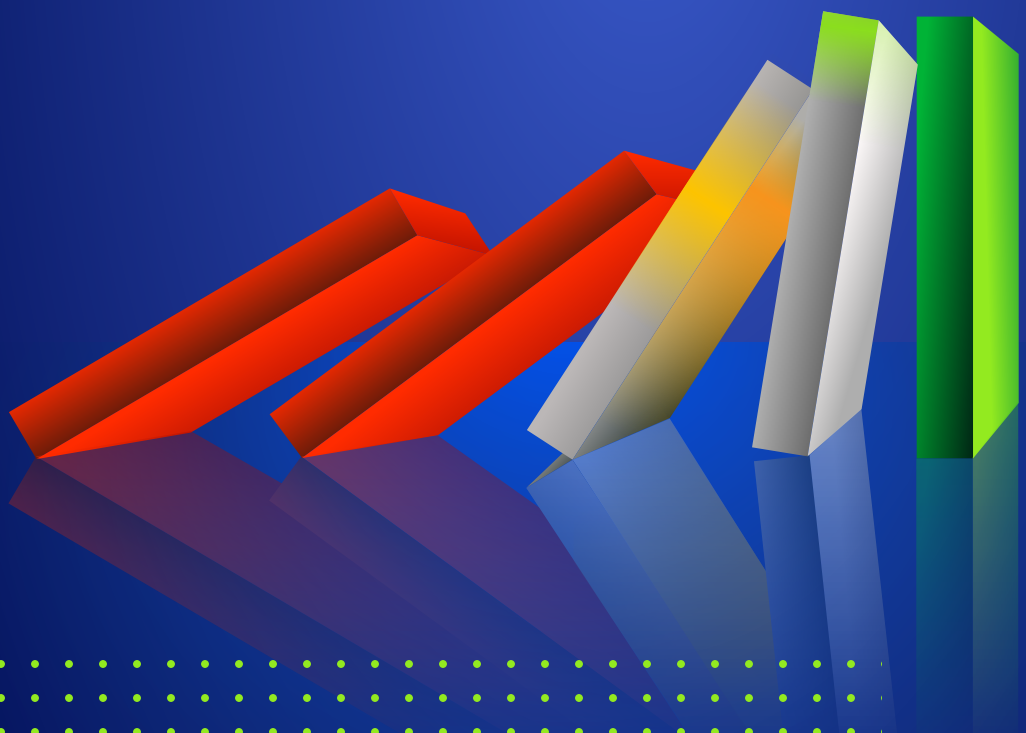
Vicepresidente de Estrategia empresarial, Veeam Software

Jeff Reichard,

Director sénior de Estrategia empresarial, Veeam Software

Chris Hoff,

Director de marketing de Protección de datos y ransomware, Veeam Software



Índice de contenidos

Las empresas no pueden evitar un ciberataque 2

Crear un framework para conseguir una recuperación resiliente 3

Mejores prácticas de Veeam contra el ransomware y funcionalidades exclusivas 4

Su última línea de defensa es un backup seguro 4

1. Inmutabilidad confiable 5
2. Verificación del backup 7
3. Regla 3-2-1-1-0 7
4. Recuperación instantánea a gran escala 8
5. Recuperación segura de datos 9
6. Orquestación del DR 10

Conclusión 11

Productos de Veeam para su estrategia de mitigación del ransomware 11

Acerca de Veeam Software 11

Acerca de los autores 12

© 2022 Veeam Software. Información Confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

Las empresas no pueden evitar un ciberataque

El crecimiento y evolución del ransomware es una de las tendencias más destructivas de la última década. Esta explosión ha llevado al ransomware de ser un delito económico, a convertirse en un delito con graves implicaciones para la seguridad a nivel mundial. La OTAN, el G7 y el gobierno federal y ejército de los Estados Unidos han reconocido recientemente la gravedad de la amenaza del ransomware y la necesidad de contar con una respuesta coordinada a gran escala por parte de la administración y la industria.

Dar una respuesta coordinada de la administración y la industria requiere tiempo. Pero mientras tanto, las organizaciones, con independencia de su tamaño, necesitan proteger en la actualidad a sus clientes, a sus integrantes y a ellas mismas. Afortunadamente pueden darse pasos concretos con las herramientas y marcos de seguridad actualmente disponibles.

El nivel de sofisticación y capacidad de adaptación del ransomware y otras ciberamenazas actuales requieren de una defensa ágil por capas. Sin embargo, todavía existen muchas organizaciones que siguen manteniendo productos de seguridad que están orientados a un único vector de ataque, que puede ser superado fácilmente. A los problemas ya inherentes de la tecnología, se le suma además la carencia de conocimientos de seguridad del personal. Un reciente estudio estima que el número de puestos de seguridad sin cubrir en todo tipo de organizaciones en todo el mundo supera los tres millones. Los problemas de personal van mucho más allá de las capacidades técnicas para saber aplicar las políticas y generar consistencia y proporcionar de esta manera, una forma de medir la efectividad general de su organización. Estos vacíos en el personal, los procesos y la tecnología facilitan más que nunca que los ciberdelincuentes más sofisticados puedan atacar sus datos.

Las organizaciones no pueden evitar un ciberataque, pero necesitan dar los pasos necesarios para estar preparados y proteger de manera eficiente sus datos cuando se produce un ataque.

Crecimiento del ransomware de 2016 a 2021

Coste global: de 325 millones a 20 000 millones de dólares USD

Frecuencia: de cada dos minutos a cada 11 segundos

Innovación: Bitcoin, ransomware-as-a-service, extorsión doble/triple

© 2022 Veeam Software. Información Confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

Crear un framework (marco) para conseguir una recuperación resiliente

Los programas de seguridad más eficaces empiezan con una estructura que permita entender qué habría que proteger y cuál sería el coste para el negocio en caso de que estos activos se perdieran, y poder determinar de esta forma cómo implementar la protección . Muchas organizaciones comienzan su andadura en el terreno de la seguridad intentando proteger cada activo de la misma forma y con el mismo nivel de importancia, pero a medida que crece se aplican mejores prácticas que permiten clasificar los riesgos y definir y medir mejor la respuesta. A medida que se implementan los marcos, los equipos de seguridad pueden madurar y comprender las amenazas a las que se enfrentan, así como las metodologías usadas por sus atacantes, lo que permite a los equipos defenderse de los ataques y recuperarse rápidamente en caso de que un ataque consiga su objetivo. Este enfoque organizado también ayuda a justificar las inversiones en materia de ciberseguridad, ilustrando claramente los resultados de esas inversiones. Y el proceso es iterativo, lo que permite una implementación por fases y el aprendizaje de los ciclos de implementación anteriores.

Sin una forma estructurada de gestionar el riesgo de la ciberseguridad, sería sencillo centrar todos los esfuerzos en defensas basadas en la detección, como firewalls y soluciones antivirus, que descuidarían los procesos y herramientas que son obligados para responder y recuperar de una manera eficiente a un ataque que alcance su objetivo. Dicho de otra manera, el mejor ataque es una defensa sólida que incluya una estrategia consolidada para hacer backup y proteger sus datos y cargas de trabajo. La posibilidad de contar con backups correctos es la última línea de defensa contra los ciberataques, y puede constituir el factor decisivo para evitar la interrupción del negocio, la pérdida de datos y el pago de un costoso rescate. A tal fin hemos confeccionado esta guía con las mejores prácticas para ofrecer consejos del mundo real sobre la protección de sus datos.

© 2022 Veeam Software. Información Confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

Mejores prácticas de Veeam contra el ransomware y funcionalidades exclusivas

Desde 2019, cada versión de la plataforma Modern Data Protection de Veeam® ha proporcionado funcionalidades importantes de ciberresiliencia y protección segura frente a ransomware, lo que ha ayudado a las organizaciones a recuperarse de forma confiable de cualquier ciberataque en cuestión de minutos. Nuestro enfoque basado en software le ofrece la flexibilidad para mantener el almacenamiento protegido e inmutable on-premises y en la nube sin sufrir el bloqueo del hardware propietario. Estas mejores prácticas le permiten disponer de una protección adecuada que garantice la prestación de un backup y restauración fiable para sus servicios críticos de infraestructura y asegurar que sus datos estarán ahí cuando los necesite.

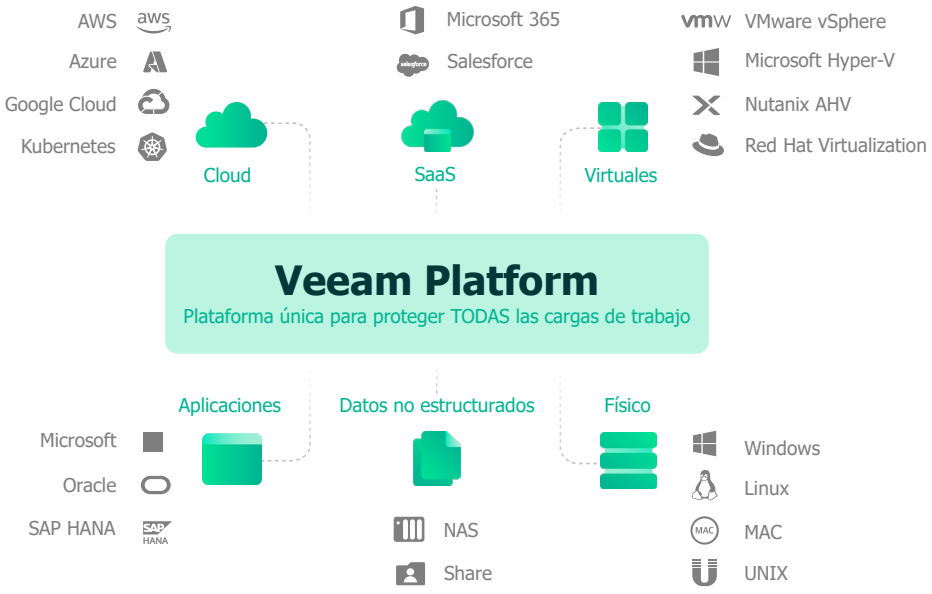
Su última línea de defensa es un backup seguro

La solución de disponibilidad implementada debería ser capaz de proteger todo el abanico de cargas de trabajo, ya sean físicas, virtuales o basadas en un contenedor. Con independencia de si las cargas de trabajo son implementadas on-premises, en la nube con IaaS o como SaaS, los datos de misión crítica ahora se alojan en diferentes ubicaciones, y necesitan ser portables para responder a requisitos futuros. La plataforma de protección deberá tener la capacidad de ampliarse o reducirse, en función de los requisitos y cargas de trabajo que se están protegiendo. La solución de backup debería ser capaz de capturar los datos a través de multitud de métodos, incluido el backup, replicación, continuous data protection (CDP) e integraciones con cabinas de almacenamiento.

Veeam ofrece una arquitectura de almacenamiento definida por software (SDS) escalable horizontalmente. En la parte de front-end, Veeam puede ampliarse fácilmente para asimilar más datos a medida que cambian sus volúmenes de backup o necesidades de rendimiento. Por el lado del back-end, un repositorio Scale-out Backup Repository™ (SoBR) es una construcción definida por software que reúne diferentes tipos de dispositivos de almacenamiento para los datos de backup. A través del motor de políticas de Veeam, los datos pueden ubicarse en los dispositivos más adecuados, que incluyen almacenamiento de conexión directa (DAS) on-premises, appliances de deduplicación, almacenamiento conectado a la red (NAS), almacenamiento de objetos y la nube; y que son gestionados automáticamente con el tiempo o a través de un proveedor de servicio.

La plataforma de Veeam proporciona todas estas funcionalidades, que permiten contar con una solución que se escala y amplía a medida que su negocio y sus necesidades evolucionan con el tiempo. El enfoque de Veeam es modular y ampliable, sin necesidad de soluciones puntuales específicas, sin dependencias obligadas de hardware y sin la preocupación de que la solución se le quede pequeña.

Las funcionalidades de corrección de ransomware definidas por software de Veeam funcionan en cualquier infraestructura, ahora y en el futuro. No se requiere una infraestructura propietaria, lo que permite a la empresa implementar la solución en el hardware o nube que elija. La flexibilidad de la infraestructura no solo permite a la organización el determinar en qué hardware se va a ejecutar su solución de backup, sino que también protege sus backups frente al ransomware, independientemente de dónde residan sus datos importantes.



© 2022 Veeam Software. Información Confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

1. Inmutabilidad confiable

Los ciberdelincuentes ahora intentan de manera rutinaria el cifrado o eliminación de los backups de la organización como parte de su ataque de backup. El éxito para el adversario es aquí crítico, ya que sin los archivos de backup, la víctima deberá pagar generosamente para recuperar sus datos.

Los backups protegidos o resilientes son backups que en esencia no pueden ser destruidos por el ciberdelincuente — incluso aunque haya conseguido credenciales de administrador.

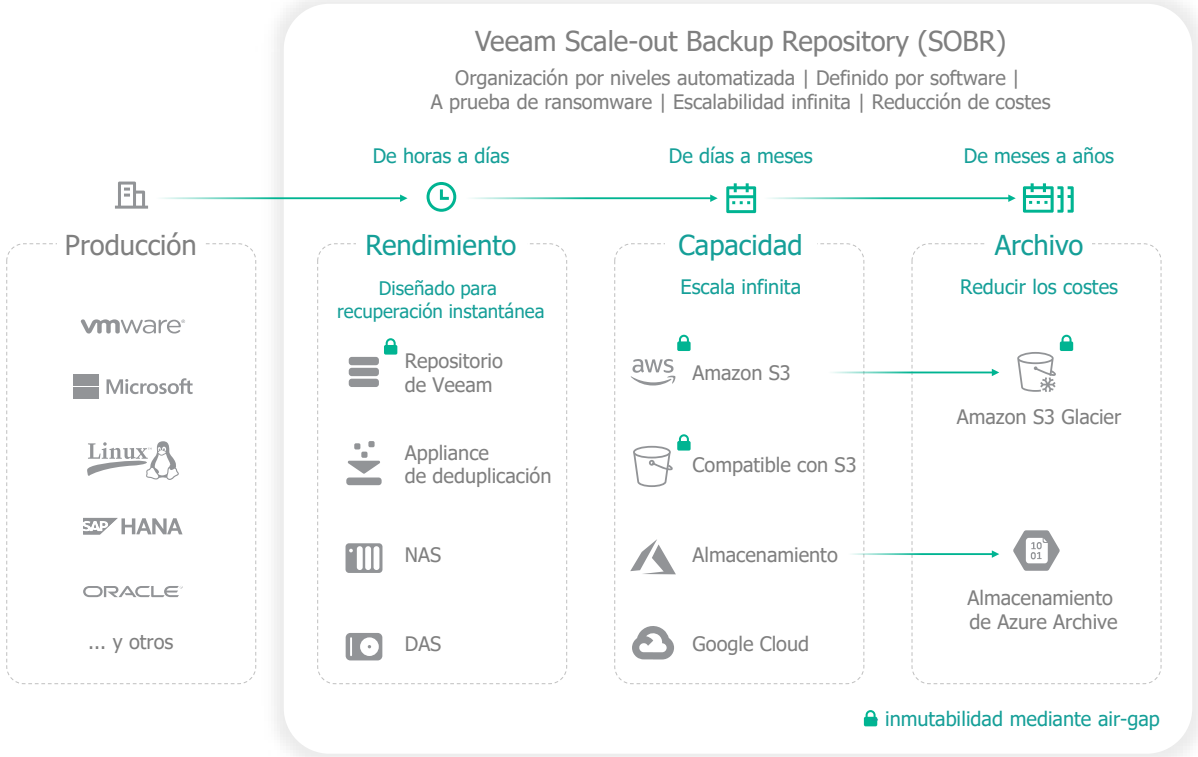
Al nivel más simple, puede conseguirse un nivel de resiliencia sólido haciendo backup a unidades extraíbles o a cintas que son retiradas de la biblioteca de cinta. El primer paso es disponer de backups desconectados y aislados (air gapped).

Veeam ofrece un enfoque a prueba de balas basado en políticas para la gestión de datos a través de diferentes opciones de almacenamiento resilientes. Las soluciones de almacenamiento certificadas de Veeam a través de nuestro extenso ecosistema de partners garantizan la *inmutabilidad* (la imposibilidad de borrar o alterar los datos durante un periodo determinado) para mejorar la resiliencia general. **Estas opciones incluyen nuestro Veeam Hardened Repository (repositorio reforzado), que proporciona una opción inmutable para realizar sus backups on-premises.** Si prefiere mantener sus datos en la nube, Veeam proporciona inmutabilidad usando AWS Amazon S3 y otros proveedores de almacenamiento de objetos compatible con S3, usando su funcionalidad de bloqueo de objetos.

Los backups guardados en almacenamiento resiliente serán una de las defensas más críticas para garantizar la protección frente al ransomware. El almacenamiento de backup resiliente significaría que puede tener una o más copias de sus datos de backup en una combinación cualquiera de los siguientes soportes:

- Backups en cinta (y eliminadas de la biblioteca o marcadas como WORM)
- Backups inmutables en S3 o almacenamiento de objetos compatibles con S3
- Medios offline y aislados o Air-gapped (por ejemplo, discos extraíbles, discos duros)
- Backups en Veeam Cloud Connect con Insider Protection (una funcionalidad de gestión de servicios)
- Backups inmutables en un repositorio reforzado

Veeam Platform incluye un conjunto completo de funcionalidades de remediación de ransomware en su producto principal que son implementables fácilmente por el cliente, y lo suficientemente flexibles para funciona con cualquier infraestructura, on-premises o en la nube.



Gestión del ciclo de vida de los datos de backup impulsada por políticas

© 2022 Veeam Software. Información Confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

Algunos clientes de Veeam buscan implementar la inmutabilidad a través de un enfoque doble o triple de inmutabilidad. Esto puede incluir el uso del Veeam Hardened Repository para los backups de primer nivel locales (on-premises), y entonces aprovechar la funcionalidad de inmutabilidad en el tier Veeam Capacity Tier gestionado automáticamente con S3 Object Lock para almacenamiento de objetos cloud u on-premises, y/o guardar automáticamente los backups a un soporte de cinta físico WORM (write one, read many); tenga en cuenta que Veeam soporta de manera nativa las cinta física sin necesidad de recurrir a integraciones de terceros.

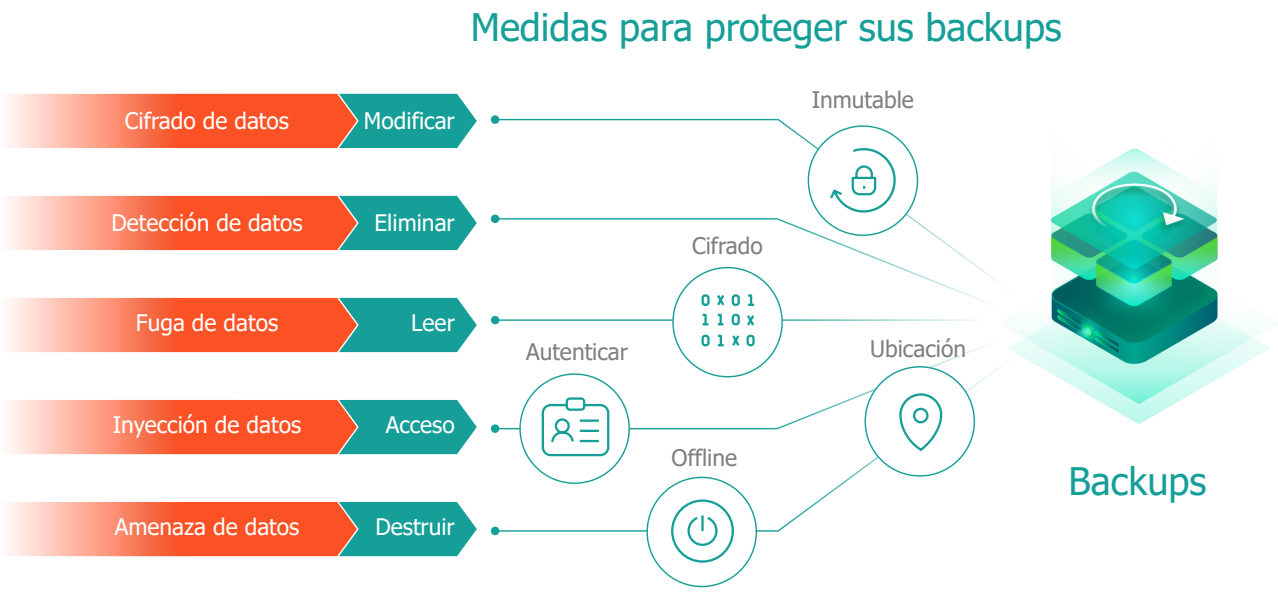
Mientras la inmutabilidad, bien sea implementada según un enfoque simple, doble o triple es de gran ayuda para enfrentarse a las ciberamenazas, es solamente el principio de una práctica de protección contra ransomware más completa.

En necesario el cifrado end-to-end para eludir la filtración de datos. Una de las ciberamenazas actuales de mayor auge es la filtración y fuga de datos, donde debe pagarse un rescate para evitar que los datos sensibles capturados sean compartidos en la dark web.

Para evitar la inyección de datos es necesario contar con un sistema de autenticación adecuado y un correcto nivel de "higiene digital" con respecto al acceso de menor privilegio. Los datos también necesitan protegerse frente a su modificación, de forma que esos registros y entradas que parecen válidos no hayan sido modificados de forma intencionada para que sean no válidos.

Entre otras mejores prácticas de higiene digital se incluyen:

- Contraseñas únicas para cada fuente de acceso. De esta forma puede garantizar que si se ha vulnerado la seguridad de una contraseña o máquina, la contraseña robada no proporcione al hacker acceso a otras cuentas.
- Un gestor de contraseñas. Un gestor de contraseñas sólido puede ayudar a gestionar toda su información de acceso, facilitando la creación y uso de contraseñas únicas y seguras.
- Autenticación Multifactor (MFA). Puede configurar la autenticación multifactor para conseguir un nivel de seguridad adicional de sus cuentas, lo que requerirá una segunda validación en cada inicio de sesión.
- Eliminar de todos los servidores los dispositivos, aplicaciones y programas no esenciales que no se utilizan.
- Gestión de parches (revisiones) — asegúrese de que todo el software, hardware y firmware que se usa, ejecuta versiones actualizadas que han eliminado o arreglado cualquier vulnerabilidad conocida.



© 2022 Veeam Software. Información Confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

2. Verificación del backup

Una estrategia de ciberdefensa integral empieza con backups que sean válidos. Contar con unos backups probados, verificados y fiables es el primer paso para tener éxito en la recuperación. Los equipos de TI están siempre ocupados, y necesitan una forma de comprobar automáticamente la integridad de los datos del backup a medida que estos son generados. Si se produce algún tipo de problema, puede capturarse otro backup mientras los datos de producción siguen disponibles, garantizando de esta forma que no se descubran problemas de disponibilidad de los datos una vez que estos datos de producción ya no están accesibles, han sido puestos en compromiso o se consideran poco fiables o faltos de integridad.

Veeam SureBackup® fue el pionero de la verificación automatizada del backup, y es una de las funciones clave en nuestras mejores prácticas de protección frente al ransomware. SureBackup pone en marcha de forma automática servidores y aplicaciones en un entorno de red aislado, y ejecuta pruebas de estado que involucran muchos medios integrados de verificación de aplicaciones, como la ejecución de comandos SQL o de Active Directory específicos para verificar la integridad de la aplicación. Esta capacidad para hacer pruebas automatizadas puede ampliarse y personalizarse para adaptarse a sus requisitos, y pueden programarse para que se ejecuten cuando crea que es el momento más propicio, enviando posteriormente un informe de estado a su buzón de correo una vez que las pruebas hayan finalizado.

3. Regla 3-2-1-1-0

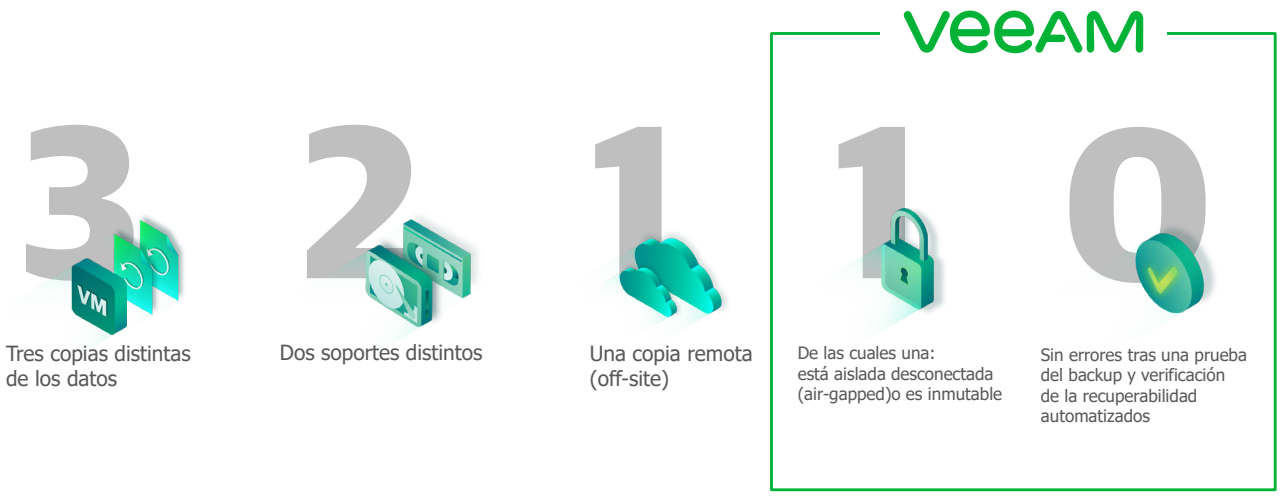
Veeam recomienda seguir la regla 3-2-1-1-0 del backup, que representa nuestra mejora a la bien conocida regla 3-2-1 de la industria.

Durante muchos años, Veeam ha propugnado la Regla 3-2-1 como una estrategia general de gestión de datos. La Regla 3-2-1 recomienda que debe haber al menos tres copias de datos importantes, en al menos dos tipos de medios diferentes, con al menos una de estas copias en un almacenamiento externo (offsite). La Regla 3-2-1 no exige o requiere ningún tipo de hardware en especial y es lo suficientemente versátil como para abordar casi cualquier escenario de fallo.

Como la amenaza del ransomware ha avanzado, Veeam ha puesto mayor énfasis en que haya "una" copia de los datos que sea ultra resiliente (es decir, que sea una copia aislada o air-gapped, esté desconectada o sea inmutable). Esta recomendación es fundamental para poder protegerse frente al ransomware.

La aplicación moderna de la regla 3-2-1-1-0 aborda la necesidad de una copia protegida, y es uno de los conceptos más importantes que puede implementar una organización para estar mejor preparada y defenderse frente a las ciberamenazas.

Se necesitan copias offline de los datos para combatir las amenazas internas, que incluyen la destrucción de los datos. Las amenazas internas son una preocupación en aumento, y algunas consultoras de analistas declaran que la gran mayoría de ciberamenazas de los próximos tres años podrían provenir de los propios empleados de la empresa.



© 2022 Veeam Software. Información Confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

4. Recuperación instantánea a escala

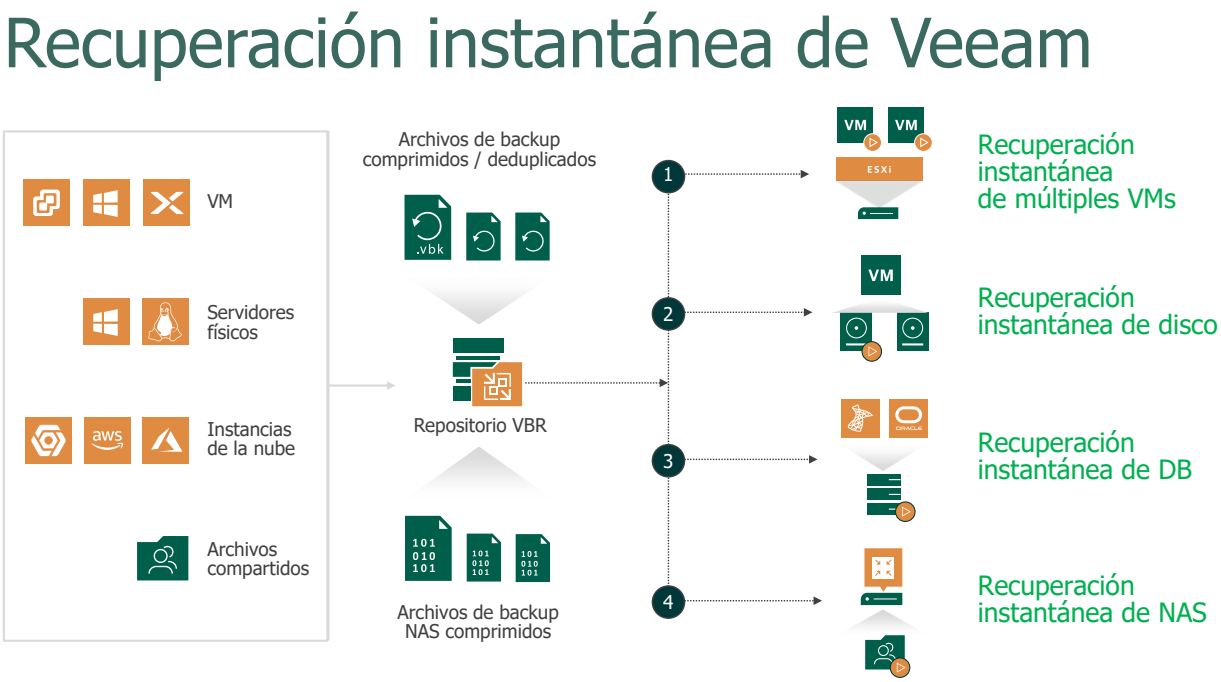
Antes de la llegada del ransomware, las organizaciones normalmente solo restauraban entre el 3 y 5 % de sus datos de backup durante un periodo de un año. Pero en un ataque de ransomware, el 100 % de sus datos de producción pueden quedar cifrados o contaminados con malware, y necesita recuperarlos todos de vuelta y rápidamente. El acceso rápido a los datos es esencial, y su objetivo es más el de reanudar todas las operaciones vitales que el de restaurar.

Veeam fue el precursor de la recuperación instantánea de los datos en 2010 y desde entonces ha refinado y ampliado esta capacidad. Actualmente las soluciones de Veeam se han optimizado para restaurar rápidamente múltiples máquinas de forma simultánea, para abordar incluso las necesidades de recuperación de las grandes empresas.

Veeam proporciona recuperación instantánea de los datos:

- Sin necesidad de appliances propietarios de costo elevado o unidades de estado sólido
- Sin limitarse únicamente a los datos de backup más recientes
- Proporciona la capacidad de recuperar archivos y cargas de trabajo físicas y virtuales a un entorno virtualizado (como VMware vSphere, Microsoft Hyper-V, y Nutanix AHV), e incluso migrar de un hipervisor a otro de forma automática, con tan solo dos clics.
- Proporciona la capacidad de recuperar archivos y servidores físicos y virtuales a un entorno en la nube (como AWS, Azure y Google Cloud Platform), con tan solo dos clics
- Proporciona la posibilidad de recuperar al instante aplicaciones empresariales clave, como bases de datos Oracle y SQL Server para su uso inmediato
- Proporciona la capacidad de devolver todo el almacenamiento conectado a la red (NAS) y los archivos de recursos compartidos a un estado bueno conocido, antes de la infección de forma que su negocio pueda volver a sus operaciones normales rápidamente

La recuperación instantánea de los datos, que puede aprovechar el uso de un formato de datos portable para proporcionar acceso a los datos desde varias plataformas, garantiza una recuperación rápida, cuándo y dónde lo necesite. Desde AHV, Hyper-V, o vSphere a entornos físicos de Windows o Linux, a Azure, AWS o GCP, Veeam Platform tiene lo que necesita.



© 2022 Veeam Software. Información Confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

5. Recuperación segura de datos

El tiempo de permanencia o espera del ransomware (el tiempo que un adversario está en la red de la víctima antes de activar un ataque) puede ser de varios meses. Por este motivo, necesita la automatización para garantizar que nunca restaura el malware nuevamente en su entorno limpio o nuevo.

Uno de los aspectos más versátiles de los trabajos de SureBackup (descrito anteriormente en el punto 2) es la capacidad para dejar el trabajo en ejecución de modo que puedan realizarse tareas de verificación y análisis forenses adicionales en el sistema desde el punto de restauración del backup. Esto puede incluir el llevar a cabo una inspección manual para ver si la amenaza del ransomware permanece en su lugar, investigando para ello archivos específicos.

Basándose en la capacidad de recuperación instantánea mencionada anteriormente, Veeam se integra con las principales soluciones antimalware para ofrecer un proceso de recuperación automatizado que verifique y limpie datos de backup infectados, garantizando que los datos de backup recuperados al entorno de producción no poseen ciberamenazas, y eliminar de esta forma la posibilidad de reinfección.

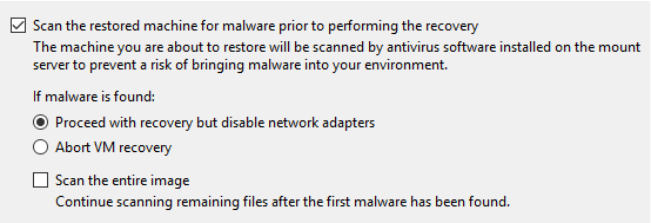
Veeam Secure Restore proporciona a los usuarios un paso opcional de análisis antivirus totalmente integrado como parte de cualquier proceso elegido de recuperación. Esta característica aborda los problemas asociados al manejo de malware malicioso, proporcionando la capacidad de garantizar que cualquier dato de la copia que quiere o necesita recuperar al entorno de producción, se encuentre en buen estado y no posea malware. **Secure Restore fue otro de los primeros métodos de la industria, pendiente de patente, para remediar un ataque proveniente de malware oculto en sus datos de backup.** Secure Restore ofrece tranquilidad adicional para saber que una amenaza ha sido neutralizada de manera adecuada y que ya no existe dentro de su entorno.

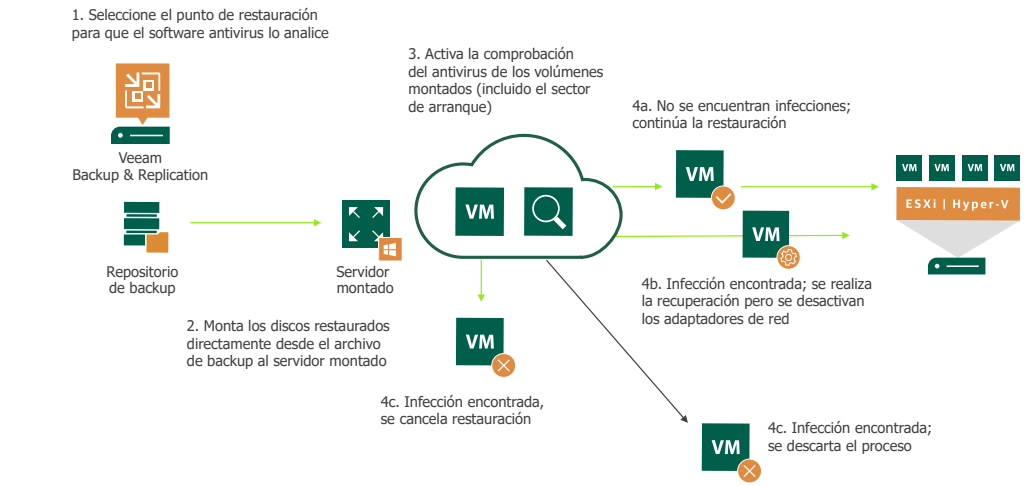
Secure Restore es totalmente configurable a través de PowerShell, lo que significa que si automatiza los procesos de recuperación mediante la integración con una solución o portal de un tercero, será capaz de aprovechar esta funcionalidad para garantizar que las amenazas no vuelven a introducirse en su entorno de producción.

Esta avanzada funcionalidad es muy útil para:

- Detectar ransomware "durmiente" en los datos de backup e invocar la corrección del software antivirus para desinfectar los datos antes de que vuelvan a copiarse al entorno de producción.
- Verificar los backups desde ubicaciones con un menor control de TI, como oficinas o sucursales remotas (ROBO), antes de restaurarlos al entorno con los datos primarios
- Analizar los datos del backup con soluciones antivirus adicionales para detectar mejor malware extraño o de día cero

Al igual que con el resto de funcionalidades de Veeam Platform, Secure Restore puede implementarse rápidamente y configurarse con un par de clics fácilmente:





© 2022 Veeam Software. Información Confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

6. Orquestación del DR

No se equivoque, los ciberataques son una catástrofe. En caso de una emergencia, su equipo necesita resultados automatizados que puedan repetirse. Su kit de herramientas debe permitir realizar pruebas y auditorías periódicas de la velocidad a la que podría recuperar tras un desastre, incluyendo las pruebas automatizadas del servidor y la accesibilidad de las aplicaciones y su capacidad de uso tras la restauración. Y el proceso de las pruebas y sus resultados deberían documentarse por sí solos para satisfacer a la dirección y a auditores de seguridad externos.

La solución de Veeam, líder de la industria, **Veeam Disaster Recover Orchestrator** (VDRO), **le permite automatizar por completo y documentar flujos de trabajo complejos, que incluyen las pruebas de recuperación a gran escala y no disruptivas, junto con la documentación dinámica de los procesos.** La documentación de respuesta/recuperación ante un incidente puede también actualizarse con información que no proviene de Veeam, como por ejemplo las listas de contactos y otra información de misión crítica necesaria para agilizar la respuesta.

Recuperación confiable

- Orquestación fiable y escalable
- Centrada en las aplicaciones

Pruebas automatizadas

- No disruptivas
- Programado y bajo demanda
- Controles de disponibilidad

Documentación dinámica

- Registros de auditoría
- Informes de cumplimiento
- Seguimiento de cambios integrado
- Remediación proactiva

La mayoría de organizaciones cuentan con diversos tipos de planes de Continuidad de negocio (BC) y Recuperación ante desastres (DR). Aquí se dan unos cuantos ejemplos:

- Fallo a nivel de aplicación
- Fallo a nivel del sitio
- Fallo de un componente de la infraestructura
- Aplicaciones de misión crítica
- Aplicaciones de desarrollo/prueba

De igual forma que la verificación automatizada de los backup es importante en el caso de SureBackup en las operaciones diarias de backup, también lo es la comprobación periódica de su plan general de recuperación ciberresiliente. Tras crear un plan de recuperación, lo más importante que puede hacer es probarlo. Necesita saber si el plan que ha desarrollado funciona. Existe la tendencia de no probar por completo los planes de recuperación ante desastres, o no probarlos de ninguna forma. En el mejor de los casos, la mayor parte de las organizaciones prueban sus planes de DR de manera parcial una o dos veces al año.

Es muy importante realizar pruebas constantemente, especialmente porque las aplicaciones suelen cambiar continuamente. Para poder responder a las modificaciones y desviaciones en la configuración, los planes de recuperación deben actualizarse cada vez que se produce un cambio en la aplicación, como por ejemplo añadir más servidores para conseguir mayor capacidad, o eliminar servidores antiguos. Al hacer las pruebas hay que asegurarse de que se presta especial atención o lo que no ha salido como cabía esperar. Este es el único camino posible para que su plan de recuperación ante desastres mejore. El propósito real de una prueba es descubrir si su plan funciona o no.

La ciberresiliencia y la corrección del ransomware necesita formar parte de su plan general de recuperación ante desastres. Una de las formas más claras con las que puede prepararse para responder ante incidentes de ciberseguridad es elaborar un plan de respuesta ante incidentes. Crear un plan de respuesta ante incidentes bien definido le permitirá perfilar los procesos para detectar, comunicar, controlar y remediar los incidentes de seguridad de forma que los empleados sepan cómo responder antes eventos de ciberseguridad en caso de que estos se produzcan.

Es más, es necesario que este plan pueda probarse de forma automatizada, actualizarse su documentación dinámicamente con información crítica, y permitir la integración con otras herramientas y flujos de trabajo necesarios que garanticen que es posible la reanudación de las operaciones críticas del negocio.

Pruebas de DR y recuperación de sitios con un solo clic

Veeam Disaster Recovery Orchestrator

© 2022 Veeam Software. Información Confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

Conclusión

Los datos de una empresa son su activo más valioso; sin embargo, el ransomware es una amenaza en auge que afecta a organizaciones de todos los tamaños, industrias y ubicaciones geográficas, y que pone en peligro sus datos más importantes. Es indispensable que las empresas sigan mejorando sus programas de seguridad para garantizar que los datos están protegidos adecuadamente, y que todas las empresas dispongan de la capacidad para recuperar su operativa tras un incidente de forma rápida y segura. Desarrollar un programa de seguridad integral requiere la combinación de personal, procesos y tecnología de forma que se centren en la mejora continua y proporcionen la mejor defensa posible. No importa la metodología que elijan las empresas, el framework necesita definir resultados que puedan medirse y que permitan a los equipos de TI defenderse frente a los ataques y recuperar rápidamente en caso de que un ataque resulte fructífero.

La respuesta ante amenazas como el ransomware requiere de la implementación de una estrategia de protección y corrección integral. El amplio conjunto de funcionalidades de mitigación de ransomware de Veeam proporciona las funciones más completas del mercado y la mayor experiencia para garantizar que los datos estén disponibles durante una crisis. Logramos esto tomando un enfoque basado en software que le ofrece la flexibilidad para mantener el almacenamiento protegido e inmutable on-premises y en la nube sin sufrir el bloqueo de hardware propietario. Con la implementación de la moderna plataforma de protección de datos de Veeam, y el seguimiento de las mejores prácticas, Veeam puede ayudar a su organización a alcanzar la resiliencia digital, que reducirá al mínimo el tiempo de inactividad tras un ataque de ransomware, usando procesos totalmente automatizados para conseguir una restauración sin ransomware y una orquestación del DR con independencia de dónde residan sus datos.

No importa si sus datos residen localmente (on-premises) o en la nube, la clave es contar con un conjunto completo de funciones de protección contra ransomware. Trasladar estas mejores prácticas a su programa de seguridad, simplifica la respuesta a los ciberataques y evita la pérdida de datos o el pago de costosos rescates.

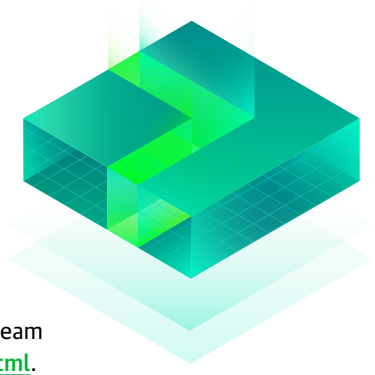
Acerca de Veeam Software

Veeam® es el líder en soluciones de Backup, Recuperación y Gestión de datos que ofrecen Modern Data Protection™. Ofrecemos una plataforma única para entornos físicos, cloud, virtuales, SaaS y de Kubernetes. Nuestros clientes tienen la certeza de que sus aplicaciones y datos están protegidos y siempre disponibles con la plataforma más sencillas, flexible, confiable y avanzada de la industria. Veeam protege a más de 400 000 clientes en todo el mundo, incluidas más del 82 % de las empresas Fortune 500 y más del 60 % de las Global 2000. El ecosistema global de Veeam incluye más de 35 000 partners tecnológicos, resellers y proveedores de servicios, y Alliance Partners y posee oficinas en más de 30 países. Para obtener más información, visite www.veeam.com/es-lat o siga a Veeam en LinkedIn @veeamsoftwareyTwitter@veeam.

Productos de Veeam para su estrategia de mitigación del ransomware

Productos de Veeam para su estrategia de mitigación del ransomware

- Veeam Backup & Replication
- Veeam ONE
- Veeam Disaster Recovery Orchestrator
- Veeam Backup *for AWS*, *Azure*, y *Google Cloud*
- Veeam Backup *for Microsoft 365*
- Kasten K10 by Veeam



Puede encontrar más información sobre las funcionalidades frente al ransomware de Veeam en este sitio web específico: https://www.veeam.com/es-lat/ransomware-protection.html.

Encontrará un documento técnico más largo y detallado con las mejores prácticas contra ransomware y un tratamiento más en profundidad de las funcionalidades de ciberseguridad de Veeam en: https://www.veeam.com/wp-protection-yourself-from-ransomware.html?wpty.

© 2022 Veeam Software. Información Confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

Acerca de los autores

Dave Russell es un veterano que posee 32 años de experiencia en la industria del almacenamiento, y desde su cargo de Vicepresidente de Estrategia de producto de Veeam, es el responsable de impulsar programas estratégicos de productos y comercialización, con los que lidera la participación en la industria y evangeliza la visión que tiene Veeam de la protección moderna de datos. Antes de Veeam, desempeñó el cargo de Vicepresidente y analista distinguido en Gartner durante 13 años, y dedicó 15 años en desarrollo de producto de IBM para el backup y recuperación de sistemas mainframe y abiertos.

Jeff Reichard es Director sénior de Estrategia empresarial en Veeam, donde se centra en cuestiones de gestión de riesgos, cumplimiento y relaciones comerciales. Jeff posee 25 años de experiencia en soluciones de protección de datos/disponibilidad, continuidad de negocio y cumplimiento de normativa reguladora. Sus responsabilidades anteriores abarcan desde el diseño de soluciones de backup de datos y SAN, a la ingeniería de sistemas y dirección al servicio de clientes empresariales y de la administración pública. Antes de llegar a Veeam, Jeff dirigió recientemente el equipo SE civil federal de Commvault. En Veeam, Jeff trabaja codo con codo con partners, clientes y analistas de la industria para llevar a cabo una misión evangelizadora de la visión de Veeam para la gestión de datos en la nube y la transformación digital.

La carrera de Chris está profundamente arraigada en el campo de la ciberseguridad y le respaldan más de 15 años de experiencia técnica. En la actualidad dirige las iniciativas de marketing de soluciones de seguridad y protección de datos en Veeam. Antes de forma parte del equipo de Veeam, Chris ha desempeñado diversos puestos en ingeniería, ventas y gestión de producto. A lo largo de su carrera profesional, ha ayudado a numerosas organizaciones a gestionar los riesgos informáticos mediante el diseño de soluciones que se alinean con los frameworks, programas y exigencias de cumplimiento normativo de la industria.

https://www.infosecurity-magazine.com/news/cybersecurity-skills-shortage-1/

Las certificaciones técnicas para el almacenamiento inmutable llegaron como respuesta al mundo de la regulación normativa en el sector financiero. Numerosas normas gubernamentales están diseñadas para garantizar que las organizaciones reguladas conserven copias inalteradas de los registros financieros durante un periodo definido (por ejemplo, en EE.UU., véase la norma SEC 17a-4(f), norma FINRA 4511 y norma CFTC Rule 1.31 (c)-(d)). Afortunadamente, las mismas certificaciones de control que garantizan la rectitud de las entidades financieras, pueden garantizar también que los datos de backup no puedan editarse y sean inalterables.

Ver https://www.veeam.com/blog/hardened-repository-passes-compliance.html para consultar las últimas certificaciones en materia de cumplimiento de Hardened Linux Repository de Veeam

© 2022 Veeam Software. Información Confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.