Resiliencia de datos Zero Trust (ZTDR)

Arquitectura de backup y recuperación de datos segura
Un enfoque pragmático para implementar el modelo Zero Trust

Descripción general

Las organizaciones de todos los tamaños y de todos los sectores comprenden la importancia de Zero Trust para garantizar la seguridad de sus datos y de su negocio. Sin embargo, el modelo Zero Trust actual todavía no se ha aplicado al backup y la recuperación de datos de manera significativa. El concepto de ampliar los principios de confianza cero al backup y la recuperación de datos se corresponde con la naturaleza holística de la ciberseguridad. La protección de la información sensible implica algo más que la seguridad perimetral.

Para abordar este desafío, Veeam colaboró con el experto en seguridad Zero Trust, Jason Garbis de Numberline Security, en el Marco de Resiliencia de Datos Zero Trust, que está diseñado para minimizar el riesgo, fortalecer la protección de los datos y revolucionar la postura de seguridad de una organización. Este marco se basa en el Modelo de Madurez Zero Trust (ZTMM) de la Agencia de Seguridad de Infraestructuras y Ciberseguridad (CISA) y amplía los principios fundamentales de ZTMM a un escenario de backup y recuperación. El Marco de Resiliencia de Datos Zero Trust implica que nunca se asume la confianza y que las medidas de seguridad se aplican de forma coherente a lo largo de todo el ciclo de vida de los datos, incluido el proceso de backup y recuperación; es un modelo práctico que ayudará a los equipos de TI y de seguridad a reducir significativamente el riesgo, mejorar la protección de datos y mejorar de manera radical la postura de seguridad de cualquier organización.

¿Desea obtener más información sobre la Resiliencia de datos Zero Trust? Descargar el white paper

El enfoque de Veeam para el modelo Zero Trust: Resiliencia de datos Zero Trust (ZTDR)

Zero Trust es la base de la estrategia de seguridad de una organización y principios clave como la segmentación en los activos de datos críticos, el acceso con menos privilegios y la autenticación y autorización continuas con las mejores prácticas de Identity and Access Management (IAM) son especialmente relevantes cuando se trata de proteger los entornos de backup. Al incorporar una función de resiliencia de datos de confianza cero, las organizaciones pueden abordar los desafíos únicos que plantean las soluciones de protección de datos y garantizar una estrategia de seguridad integral para las organizaciones, independientemente de si se encuentran en las instalaciones, en la nube o en entornos híbridos.

Un concepto fundamental de Zero Trust es asumir siempre una vulnerabilidad, independientemente de la seguridad de un entorno determinado. En la metodología ZTDR, una técnica fundamental para combatir este riesgo es separar el software de administración del backup y el almacenamiento del backup en zonas de resiliencia o dominios de seguridad separados, aislando los datos del backup de cualquier amenaza al software de administración de backup, ya sean internas o externas. Veeam admite varias tecnologías para crear zonas de resiliencia con un almacenamiento inmutable y de alta seguridad (ver Figura 1).

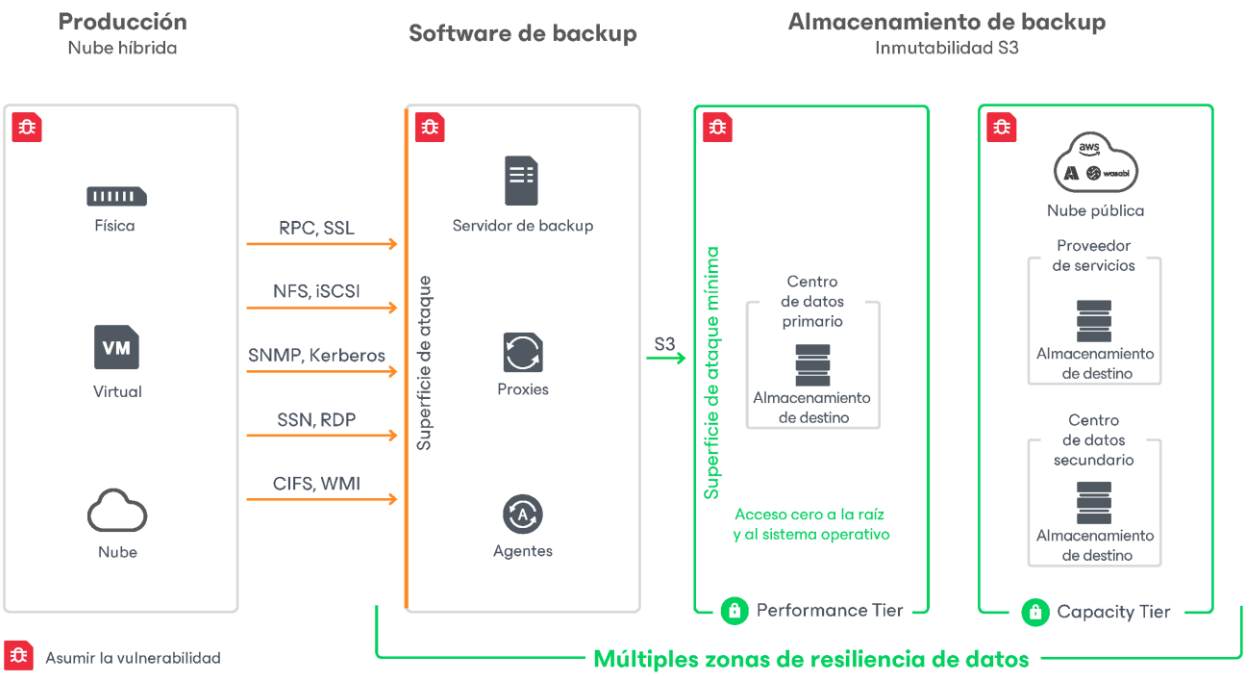

Figura 1

Debido a que las soluciones de protección de datos tienen algunos de los niveles más altos de acceso de lectura y escritura a los datos de producción en toda la organización y, a menudo, a los datos más críticos, es imperativo que el entorno de backup de una organización sea seguro y esté protegido mediante las mejores prácticas de confianza cero.

Principios de Resiliencia de datos Zero Trust

Sobre la base del Modelo de Madurez Zero Trust de CISA (consulte la Figura 2), hay consideraciones adicionales que una organización debe aplicar específicamente al pilar de datos.

Modelo de Madurez Zero Trust para CISO

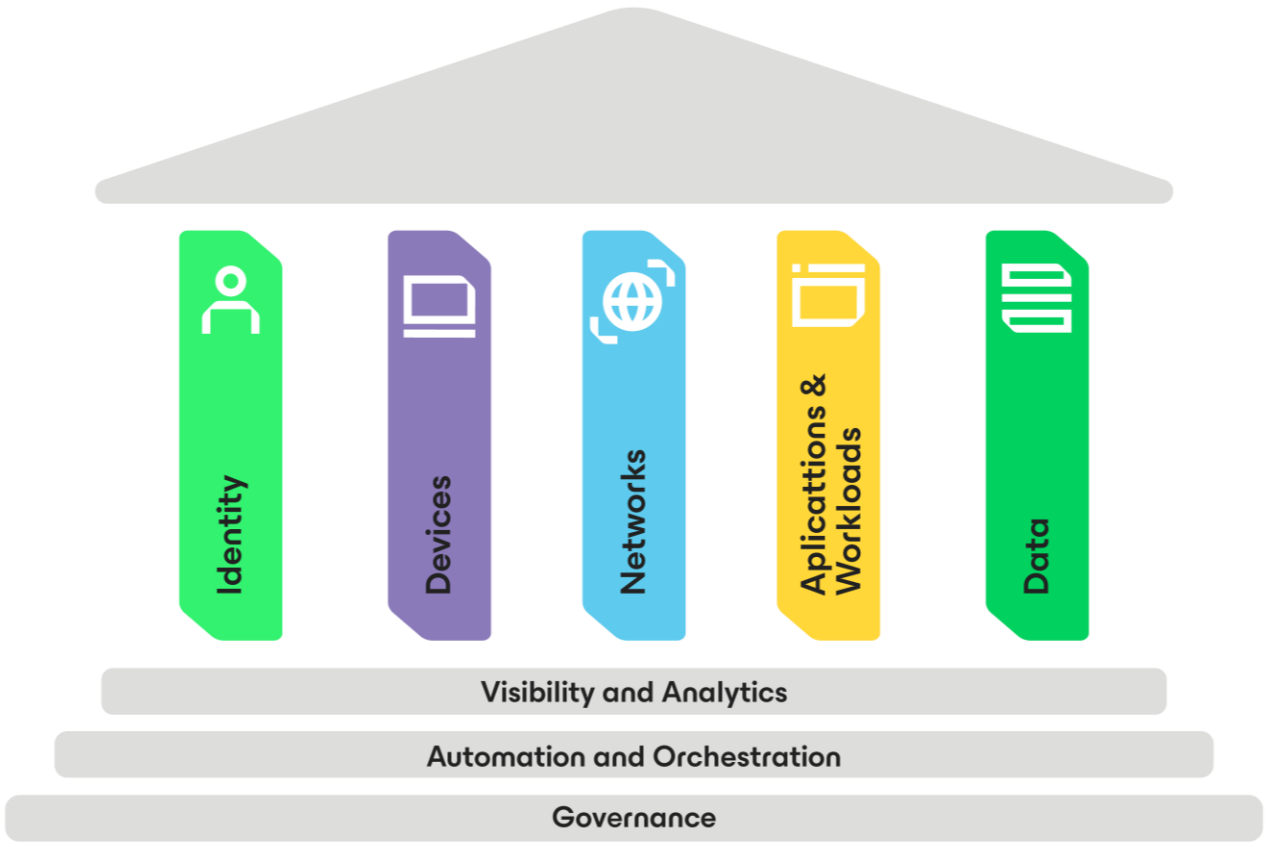

Figura 2

El artículo de investigación Zero Trust Data Resilience destaca 5 principios básicos de Resiliencia de datos Zero Trust (ZTDR) para ayudar a la estrategia general de ciberresiliencia de la organización, garantizando la protección de los activos de datos críticos frente a las amenazas cibernéticas en continua evolución.

Acceso de privilegio mínimo

Este principio hace hincapié en conceder acceso a una persona, proceso, dispositivo o carga de trabajo que sea esencial para realizar su función prevista.

Acceso controlado para la infraestructura de backup:

- La implementación de políticas Zero Trust para controlar el acceso a la infraestructura de backup garantiza que solo los usuarios validados puedan establecer conexiones con la solución de backup. Este es un paso crucial para prevenir el acceso no autorizado y las posibles vulneraciones de datos.

Roles granulares de autoservicio y roles restringidos de administrador de backup:

- Proporcionar roles granulares de autoservicio y roles de administrador de backup restringidos dentro de Veeam demuestra un compromiso con el principio de privilegio mínimo. Esto garantiza que los usuarios tengan acceso solo a las funciones específicas necesarias para sus tareas, lo que reduce la probabilidad de un uso indebido involuntario o intencionado.

Mejores prácticas de Identity and Access Management (IAM)

- La aplicación de las mejores prácticas de IAM, como el uso de la autenticación multifactor (MFA), añade una capa adicional de seguridad al entorno de backup. Esta es una medida crítica para evitar el acceso no autorizado, especialmente dados los altos niveles de privilegio asociados con las soluciones de backup.

Principio de los "cuatro ojos" para la toma de decisiones operativas críticas:

- La incorporación del principio de los "cuatro ojos" para las decisiones operativas críticas garantiza que las acciones clave requieran la aprobación o verificación de al menos dos personas autorizadas. Esto añade una capa adicional de supervisión y reduce el riesgo de actividades maliciosas o erróneas.

Inmutabilidad

Incluso con un perímetro de red seguro, un concepto fundamental de Zero Trust es asumir una vulnerabilidad. La inmutabilidad de los backups es un poderoso mecanismo de defensa, ya que asegura que un actor de amenazas interno o externo no pueda modificar o eliminar datos críticos del backup.

Segmentación para minimizar la superficie de ataque y el radio de impacto:

- Segmentar el software de backup y el almacenamiento de backup en zonas de resiliencia separadas es el concepto clave de ZTDR. Esto minimiza el impacto potencial de amenazas internas o externas al aislar los componentes críticos. Asegurarse de que el software de backup no tenga permisos de nivel de gestión o al sistema operativo en el almacenamiento de backup añade una capa adicional de protección.

Varias zonas de resiliencia y regla de backup 3-2-1-1:

- Varias zonas de resiliencia de datos o dominios de seguridad proporcionan seguridad multicapa. Además, la regla de backup 3-2-1-1 es una práctica recomendada para la estrategia de backup y se alinea bien con los principios de la resiliencia de datos. Tener al menos tres copias de los datos, en dos soportes diferentes, y con al menos una copia externa y otra separada físicamente o inmutable proporciona seguridad multicapa, lo que reduce el riesgo de pérdida de datos.

Zonas de resiliencia

Un concepto central de Zero Trust para las redes es la microsegmentación para dividir los perímetros de seguridad en zonas más pequeñas, reduciendo así la superficie de ataque, el alcance del impacto de cualquier zona comprometida y el movimiento lateral de un atacante. En el caso de ZTDR, este concepto se puede aplicar mediante el uso de zonas de resiliencia de datos. Las zonas de resiliencia separan el almacenamiento de backup y aíslan el plano de control de almacenamiento del software de backup y su plano de control. Esto proporciona una línea de demarcación crítica que garantiza la supervivencia de los datos de backup incluso en el caso de que el software de backup esté en riesgo. Esto puede suceder por varias razones, incluidos los actores de amenazas internas. Un sistema de backup debe garantizar que los datos de backup puedan recuperarse de forma sencilla y rápida a partir de una instalación limpia del software de backup.

Infraestructura de producción

Infraestructura Veeam

Datos de backup autónomos

Inmutable | Cifrado | 3-2-1-1-0

Integridad de datos y seguridad mejorada:

- Configurar un repositorio de backup compatible y establecer un periodo de retención para los backups inmutables es una medida proactiva para garantizar la integridad de los datos y una seguridad mejorada. Los backups inmutables actúan como protección contra los ataques de ransomware y otras formas de manipulación de datos.

Resiliencia del sistema

Un enfoque holístico de la seguridad informática abarca la resiliencia en todo el ecosistema, incluidas las plataformas, las herramientas, la tecnología y los procesos. Las diversas opciones de resiliencia de Veeam demuestran el compromiso de proporcionar a las organizaciones herramientas para resistir diversos tipos de interrupciones, incluida una pérdida total del sistema.

Detección de desfase temporal para backups inmutables:

- La implementación de la Detección de desfase temporal es una medida proactiva para evitar la eliminación de backups inmutables, incluso ante un NTP (Network Time Protocol) en riesgo. Esta característica mejora la seguridad y confiabilidad de los repositorios de backup, garantizando la integridad de los datos de backup críticos.

Opciones de recuperación flexibles:

- Veeam habilita opciones de recuperación flexibles, incluso para entornos diferentes, y admite implementaciones físicas y virtuales, así como entornos híbridos, para adaptarse a las diversas infraestructuras de TI que puedan operar las organizaciones. Esta flexibilidad permite a las organizaciones realizar recuperaciones rápidas: por ejemplo, de VMware en las instalaciones a AWS o Azure, o de AWS a Azure en caso de que el entorno original no esté disponible.

Opciones de restauración de datos a nivel granular:

- La flexibilidad para restaurar datos a diferentes entornos y con diferentes granularidades mejora la resiliencia general de los datos. Esta capacidad de adaptación permite a las organizaciones adaptar sus procesos de recuperación en función de las necesidades específicas de los diferentes escenarios.

Validación proactiva

La validación constante de los aspectos funcionales y de los procesos es fundamental para garantizar que los datos permanezcan protegidos y que cualquier anomalía sea detectada y tratada con prontitud.

Monitorización y validación continua:

- El énfasis en los sistemas de monitorización 7/24/365 refleja la idea de que las amenazas de ciberseguridad pueden surgir en cualquier momento. Al disponer de información en tiempo real sobre el estado del entorno, los administradores pueden detectar cualquier anomalía con antelación y permite a las organizaciones investigar y responder antes de que se produzca un posible ciberataque o pérdida de datos.

- Aprovechar herramientas como Veeam ONE para la monitorización es un enfoque proactivo para mantener la salud y la seguridad de los entornos de backup y recuperación. La capacidad de Veeam ONE para monitorizar diversos parámetros, entre los que se incluyen el uso de la CPU, la tasa de escritura en el almacén de datos, la tasa de transmisión de red y el tamaño de los backups incrementales, proporciona a las organizaciones información valiosa sobre posibles problemas.

Visibilidad end-to-end

- El concepto de visibilidad end-to-end en toda la infraestructura de protección de datos es esencial. Garantiza que las organizaciones tengan un conocimiento exhaustivo de la salud y el estado de sus sistemas de backup y recuperación, lo que les permite tomar decisiones informadas y tomar medidas rápidas cuando sea necesario.

- Como parte de la reciente versión 12.1 de Veeam, el nuevo Centro de amenazas de Veeam agrega información de toda la plataforma e infraestructura, combinándola en un panel único que destaca las amenazas, identifica los riesgos y proporciona a las organizaciones un sencillo y potente scorecard de seguridad de todo su entorno de protección de datos.

Simplicidad operativa

La importancia de la simplicidad operativa durante desastres o eventos de ciberseguridad es un reconocimiento del papel fundamental que la simplicidad desempeña en la recuperación efectiva. Cuanto mayor sea el tiempo de inactividad, mayor será el impacto en las operaciones y los resultados de una organización.

Tiempo medio de inactividad en los ataques de ransomware:

- Tal y como se recoge en el informe de tendencias de ransomware 2023 de Veeam, el tiempo medio de inactividad de un ataque de ransomware es de tres semanas. Esto subraya la urgencia y la importancia de una recuperación rápida, especialmente crítica durante situaciones de alta presión donde cada momento cuenta.

Equilibrio de herramientas, personas y procesos:

- Encontrar el equilibrio adecuado entre herramientas, personas y procesos es un desafío clave, especialmente cuando las organizaciones se enfrentan a un desastre o un ciberataque. La simplicidad operativa implica agilizar los flujos de trabajo, optimizar los procesos y garantizar que se cuenta con las herramientas adecuadas para una recuperación eficiente.

Inversión en la simplificación de las capacidades de restauración:

- Los líderes de la industria como Veeam invierten de forma proactiva en brindar capacidades de restauración abordando las complejidades de la recuperación. La capacidad para restaurar datos de una plataforma a otra y aprovechar herramientas como Recovery Orchestrator de Veeam demuestra los esfuerzos que dedican a simplificar escenarios de restauración complejos y mantiene los planes de failover actualizados, automatizados y totalmente comprobados, lo que garantiza una preparación adecuada en escenarios de alta presión.

Conozca las últimas funcionalidades de seguridad de la versión 12.1

Conclusión

A medida que nuestro panorama digital evoluciona y se expande, también lo hacen los ciberataques y las capacidades de los actores de amenazas. Como resultado, tenemos una necesidad apremiante de unificar y fortalecer la colaboración y la eficacia de TI y seguridad para proteger y defender mejor los datos, los dispositivos y las personas de nuestras organizaciones. Esta transición hacia la madurez no sucederá de la noche a la mañana, pero es imperativo que comience a suceder cuanto antes mejor. El primer paso es Zero Trust. El Modelo de Madurez de Confianza Cero (ZTMM, por sus siglas en inglés) de CISA proporciona principios básicos que son fundamentales para asegurar y proteger una organización, pero no lo cubre todo. La introducción de la Resiliencia de datos Zero Trust (ZTDR, por sus siglas en inglés) como una extensión del Modelo de Madurez Zero Trust (ZTMM, por sus siglas en inglés) de CISA es un enfoque estratégico y con visión de futuro para abordar el panorama cambiante de las amenazas cibernéticas.

La incorporación de los principios de ZTDR, que incluyen el acceso de mínimo privilegio, la inmutabilidad, la resiliencia del sistema, la validación proactiva y la simplicidad operativa, muestra una estrategia integral para asegurar y proteger los datos de la organización. Al adoptar ZTDR, las organizaciones tendrán un camino claro y concreto para fortalecer su postura de seguridad. Esto implica operaciones más eficientes y una coordinación entre los equipos de TI y de seguridad que, en última instancia, llevarán a una recuperación más rápida y segura.

Acerca de Veeam Software

Veeam, el líder del mercado mundial en protección de datos y recuperación frente a ransomware, tiene la misión de ayudar a todas las organizaciones, no solo a recuperarse de una interrupción o pérdida de datos, sino a seguir adelante. Con Veeam, las organizaciones logran una resiliencia radical a través de la seguridad de los datos, la recuperación de datos y la libertad de datos para su nube híbrida. Veeam Data Platform proporciona una solución única para entornos de nube, virtuales, físicos, SaaS y Kubernetes que proporciona a los responsables de TI y seguridad la tranquilidad de saber que sus datos y aplicaciones están protegidos y siempre disponibles. Con sede en Columbus, Ohio, y oficinas en más de 30 países, Veeam protege a más de 450 000 clientes en todo el mundo, incluido el 73% de las empresas de Global 2000, que confían en Veeam para mantener sus negocios en funcionamiento. La resiliencia radical comienza con Veeam. Más información en www.veeam.com/es o siga a Veeam en LinkedIn @veeam-software y X @veeam.