Ampliación del modelo Zero Trust al backup y recuperación de datos

Una guía práctica para profesionales de TI y seguridad

Contenido

Resumen ejecutivo

Zero Trust es una estrategia moderna y muy eficaz para proteger mejor la infraestructura de TI de nuestra empresa frente al ransomware y otras amenazas. Los sistemas de backup y recuperación de datos son fundamentales para nuestras empresas y deben incluirse en cualquier iniciativa Zero Trust.

Sin embargo, el modelo Zero Trust puede ser complicado de diseñar e implementar y, hasta ahora, no ha habido consenso sobre cómo aplicarlo mejor a los sistemas de backup y recuperación de datos.

Resiliencia de datos Zero Trust (ZTDR), un nuevo modelo introducido por Veeam y Numberline Security, sebasa en el Modelo de Madurez Zero Trust de la Agencia de Seguridad de Infraestructuras y Ciberseguridad (CISA). ZTDR amplía los principios de Zero Trust a los backups y la recuperación, lo que garantiza que las empresas puedan reducir el riesgo y cumplir sus objetivos de seguridad y resiliencia.

Siguiendo el enfoque Resiliencia de datos Zero Trust que se explica en esta guía, descubrirá qué buscar en una plataforma y arquitectura de backup y recuperación de datos, y podrá empezar de forma rápida y eficaz en su entorno.

Zero Trust: una breve introducción

Zero Trust es una estrategia de seguridad moderna basada en la idea de que no se debe confiar implícitamente en ningún usuario, dispositivo o paquete de red. Para garantizar la seguridad de los datos, el acceso a los activos de datos críticos debe estar segmentado y todas las comunicaciones deben autenticarse, evaluarse y autorizarse antes de conceder cualquier acceso. Esto debe aplicarse a cada segmento y sus datos, aplicaciones, activos o servicios.

Es un cambio significativo con respecto a las arquitecturas tradicionales de seguridad de la información, que se basaban en perímetros estáticos basados en la red, y que claramente no han logrado mantener a nuestras empresas a salvo del ransomware y los actores maliciosos.

Presentamos la Resiliencia de datos Zero Trust (ZTDR)

Los sistemas de backup y recuperación de datos son elementos fundamentales de la TI empresarial, así como objetivos frecuentes para los ataques. Deben estar asegurados de manera adecuada e integral.

Al seguir los principios de ZTDR y elegir los proveedores de backup y almacenamiento basándose en las directrices de ZTDR, su empresa obtendrá defensas más sólidas, operaciones más eficientes y una recuperación más rápida y confiable.

ZTDR amplía los principios básicos de Zero Trust

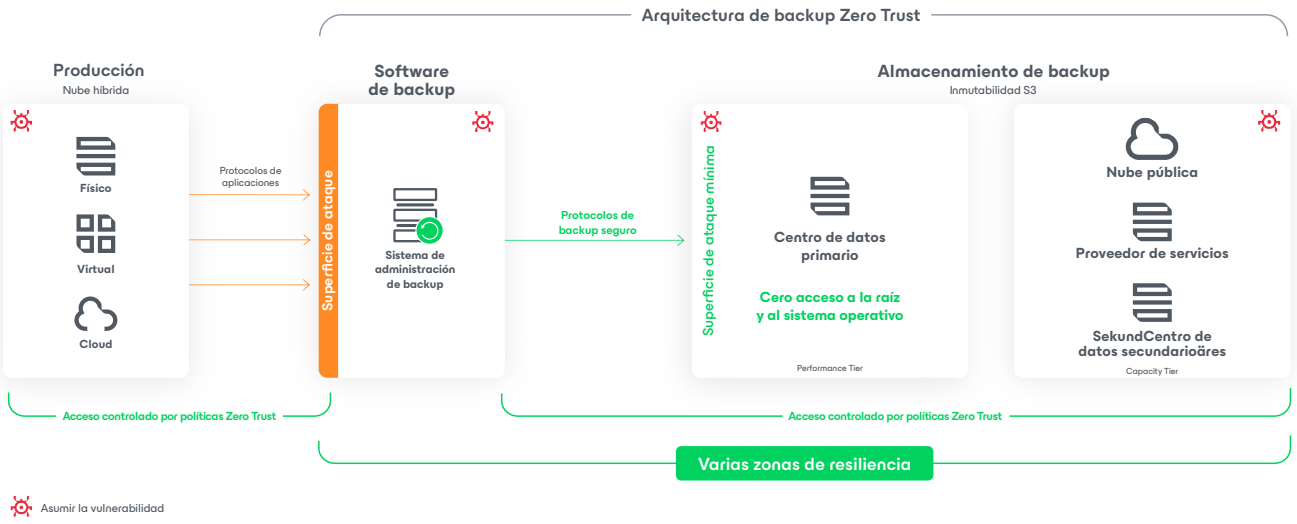
Separación del software de backup y el almacenamiento de backup	Múltiples Zonas de resiliencia	Inmutable Almacenamiento de backup
Minimizar la superficie de ataque y el radio de explosión	Regla 3-2-1 del backup	Proteja los datos de backup de modificaciones o eliminaciones
REQUISITOS DE LA SOLUCIÓN		
Busque soluciones de backup y recuperación de datos que estén diseñadas con separación entre el software de backup y el almacenamiento, y que idealmente eviten el acceso root o del OS al almacenamiento de backup. Estas funcionalidades le permitirán aplicar estrictamente los controles de acceso a través de políticas Zero Trust.	Busque soluciones de backup y recuperación de datos que soporten múltiples zonas de resiliencia, de forma que su organización pueda sobrevivir a la pérdida o al riesgo de un único sistema de backup o entorno de almacenamiento. Esto le permitirá cumplir fácilmente con las pautas de backup 3-2-1.	Busque soluciones de backup y recuperación de datos que admitan de manera fácil y eficiente un almacenamiento de backup inmutable sólido y confiable. Esto le dará la plena confianza de que sus datos respaldados están protegidos contra la eliminación o modificación, incluso en presencia de un actor malicioso.

La regla 3-2-1 para las mejores prácticas de backup:

3	2	1
3 copias de los datos, incluidos los datos de producción.	2 copias de los datos de backup en almacenamiento inmutable en zonas de resiliencia independientes.	1 copia off-site.

Arquitectura de referencia de ZTDR

Esta arquitectura de referencia de ZTDR le muestra cómo debe implementarse una plataforma Zero Trust junto con sus sistemas de almacenamiento y gestión de backups.



Primeros pasos con ZTDR

Aunque Zero Trust es un proceso, hay medidas inmediatas e impactantes que puede adoptar para mejorar la resiliencia de seguridad de su infraestructura de backup y recuperación de datos.

Esta semana:

Analice el grado de cumplimiento de los requisitos de ZTDR por parte de sus sistemas de backup y recuperación.

Tarea	Preguntas frecuentes
Hable con sus equipos de redes e infraestructura de TI sobre la segmentación de su red	• ¿Cómo está segmentada nuestra red? • ¿El software de backup y el almacenamiento de backup están segmentados en zonas de seguridad separadas? • ¿Cómo se controla el acceso hacia y desde cada segmento de la infraestructura de backup?
Evalúe si su almacenamiento de datos de backup está organizado en varias zonas de resiliencia	• ¿Seguimos las directrices del sector en torno al 3-2-1? • ¿Qué sucede con nuestros procesos de backup y recuperación si una de nuestras zonas de backup no está disponible? • ¿Qué sucede con nuestros procesos de backup y recuperación si dos de nuestras zonas de backup no están disponibles?
Determine si sus sistemas de almacenamiento de backup son realmente inmutables	• ¿Cómo documenta y garantiza su proveedor de almacenamiento la inmutabilidad? • ¿Puede un administrador malintencionado cambiar la configuración de inmutabilidad o retención mediante el acceso raíz o del SO al almacenamiento? • ¿Qué sucede si la hora del sistema se adelanta con fines malintencionados?
Valide sus procesos de recuperación	• ¿Cuál es nuestro plan de respuesta de DR? ¿Cuándo fue la última vez que lo probamos? • ¿Cuántas personas del equipo de TI o de almacenamiento pueden recuperar con éxito un sistema siguiendo los pasos documentados? • ¿Qué sucede si (persona importante X) no está disponible durante un incidente?

La próxima semana:

Valide sus procesos y herramientas, y luego planifique y genere consenso para realizar cambios a corto y medio plazo en sus procesos e infraestructura de backup y recuperación.

Tarea	Preguntas frecuentes
Evalúe su confianza y la repetibilidad de sus procesos de recuperación mediante la realización de pruebas periódicas (semanales/ mensuales)	• ¿Con qué frecuencia hacemos nuestras pruebas de recuperación? • ¿Qué aprendimos sobre las brechas en la documentación o los procesos? • ¿Cuándo podemos solucionarlos?

Tarea	Preguntas frecuentes
Comience a planificar la configuración de la red, la segmentación o los cambios en las reglas del firewall	• ¿Con quién puedo colaborar en el equipo de TI o de seguridad para analizar posibles cambios? • ¿Quién en el equipo de seguridad lidera nuestra iniciativa Zero Trust y cómo puedo apoyarla? • ¿Qué segmentación de red o cambios de infraestructura tenemos en curso?
Planifique cualquier cambio en la configuración del almacenamiento o evaluaciones de nuevos proveedores, con el fin de cerrar cualquier brecha de inmutabilidad	• ¿Cuál es nuestro proceso para evaluar y adquirir almacenamiento de backup adicional? • ¿Qué tipo de justificación financiera, de eficiencia o de riesgo tendríamos que hacer? • ¿Cómo debo obtener la aprobación para iniciar un proceso de evaluación de proveedores?
Asigne propietarios responsables para cualquier mejora en los procesos y la documentación	• ¿Quién participaría en la aprobación e implementación de los cambios en (el proceso X)? • ¿Cómo podemos fijar un plazo mutuamente aceptable para la implementación?

Próximo mes:

Comience a implementar cambios a corto plazo y comience a identificar los cambios necesarios a largo plazo.

Tarea	Preguntas frecuentes
Implemente sus procesos mejorados de recuperación ante desastres y vuelva a realizar pruebas	• ¿Cuánto mejoraron nuestros procesos de DR? • ¿Abordamos todas las brechas de proceso y documentación?
Valide e itere en la segmentación de la red	• ¿Qué áreas de la red todavía otorgan acceso amplio a y desde nuestros sistemas de backup? • ¿Cómo podemos ajustar esto para mejorar nuestra resiliencia frente al ransomware?
Implementar mejoras en la capacidad de almacenamiento, ubicaciones e inmutabilidad	• ¿Cómo de cómodos estamos con nuestra capacidad de almacenamiento de backup? • ¿Cómo de seguros estamos de que nuestros sistemas de almacenamiento de backup soninmutables? • ¿Cómo de bien estamos siguiendo la guía de mejores prácticas 3-2-1? • ¿Cómo estamos utilizando las múltiples zonas de resiliencia?

¿Qué más debería buscar?

Validación proactiva de la recuperación ante desastres

Los incidentes que requieran la recuperación de los datos respaldados van a ocurrir en momentos inesperados y probablemente en circunstancias de mucho estrés. Es importante que su organización cuente con planes y procesos de recuperación ante desastres bien entendidos, bien documentados y bien ensayados. Asegúrese también de tener un alto grado de confianza en la integridad y validez de los datos de los que se ha hecho copia de seguridad.

Simplicidad operativa

Asegúrese de seleccionar un sistema que sea lo suficientemente sencillo para que su organización pueda operar de manera fácil y segura, y que al mismo tiempo proporcione suficiente capacidad, escalabilidad y sofisticación para satisfacer plenamente las necesidades de su empresa. Esfuércese por comprender claramente la capacidad y las habilidades de su personal, de modo que las operaciones no dependan de un solo individuo o "superhéroe".

Preguntas frecuentes

¿Es Zero Trust algo que se puede comprar a un proveedor?

No, Zero Trust es algo que usted **hace**, es una estrategia de seguridad que cambia y mejora la TI, la seguridad y los resultados empresariales.

¿Zero Trust se limita a restringir el acceso y reducir la productividad de los usuarios?

No. Zero Trust consiste en eliminar todos los accesos **innecesarios** y, al mismo tiempo, mantener la productividad de los usuarios. Muchas empresas **mejoran** la productividad y la experiencia de los usuarios con Zero Trust.

¿Por qué es importante Zero Trust?

Zero Trust es la forma más eficaz de defender a nuestras empresas frente a riesgos como el ransomware, los actores maliciosos y otros. Dado el panorama actual de amenazas, tenemos la responsabilidad de utilizarlo.

¿Puede utilizar su infraestructura de seguridad actual para Zero Trust?

¡Lo más probable es que sí! Cuando se utilizan correctamente, los sistemas modernos de firewall, identidad e infraestructura pueden ayudarlo a comenzar su viaje hacia Zero Trust. Alcanzar niveles óptimos de madurez de Zero Trust puede requerir inversiones adicionales, que pueden guiarse por herramientas como la arquitectura de referencia ZTDR.

Recursos adicionales

¿Quiere obtener más información sobre Zero Trust y ZTDR?

- Visite el sitio web de Veeam para leer la investigación completa de ZTDR y conocer el enfoque de Veeam en materia de seguridad de datos y ciberresiliencia.
- Para leer el documento técnico completo de la investigación de ZTDR y obtener la perspectiva de la seguridad de Numberline al respecto, visite el sitio web de Numberline.

Acerca de Veeam Software

Veeam, el líder n.º 1 del mercado mundial en resiliencia de datos, cree que las empresas deben controlar todos sus datos cuando y donde los necesiten. Veeam proporciona resiliencia de datos a través de backup de datos, recuperación de datos, libertad de datos, seguridad de datos e inteligencia de datos. Con sede en Seattle, Veeam protege a más de 550 000 clientes en todo el mundo que confían en Veeam para mantener sus negocios en funcionamiento. Más información en www.veeam.com/es o puede seguir a Veeam en LinkedIn @veeam-software y X @veeam.

Más información: veeam.com