6 razones para realizar el backup de Microsoft Entra ID

Introducción

Microsoft Entra ID (anteriormente Azure Active Directory) desempeña un papel fundamental en una estrategia de Identity and Access Management (IAM) moderna. Sin embargo, su importancia también lo convierte en uno de los principales objetivos de los ciberdelincuentes. Con la abrumadora cifra de 600 millones de ataques dirigidos a Microsoft Entra ID cada día, los riesgos se han vuelto cada vez más complejos y dañinos, lo que plantea desafíos significativos para las organizaciones en todo el mundo.

Las amenazas son tan variadas como peligrosas. Los actores de amenazas son implacables, desde las estafas de phishing que engañan a los usuarios para que entreguen credenciales hasta los ataques de relleno de credenciales que explotan los datos robados. Las consecuencias son catastróficas:

- Los empleados pierden acceso a los sistemas críticos, lo que paraliza la productividad.
- Los clientes no pueden acceder a los servicios, lo que genera frustración y una posible pérdida de clientes.
- El tiempo de inactividad y los esfuerzos de recuperación agotan los recursos, mientras que las multas regulatorias se suman a la carga.
- La noticia de una violación se propaga rápidamente, erosionando la confianza con los clientes, socios y partes interesadas.
- Las filtraciones de datos a menudo conducen a infringir regulaciones como RGPD o HIPAA, lo que resulta en fuertes sanciones.

Recuperarse de un ataque no es hazaña sencilla. Exige tiempo, recursos y una estrategia clara para restaurar las operaciones y reconstruir la confianza. Y aunque Microsoft proporciona características de seguridad sólidas, la responsabilidad de proteger sus datos de acuerdo con el modelo de responsabilidad compartida recae en las organizaciones. Las amenazas de seguridad son solo una de las razones por las que necesita proteger los datos de Microsoft Entra ID. En este e-book se muestran y explican muchas más.

1

Amenazas para la seguridad

El riesgo siempre presente de los ciberataques requiere de defensas sólidas para protegerse contra el acceso no autorizado y las posibles infracciones.

2

Cumplimiento

Las prácticas adecuadas de administración de datos garantizan el cumplimiento de los estándares locales, nacionales y globales.

3

Borrados accidentales y errores de configuración

El error humano puede conducir a una pérdida masiva de datos e interrupciones significativas.

4

Limitaciones de la papelera de reciclaje

Depender de las herramientas integradas, como la papelera de reciclaje, es insuficiente para llevar a cabo una recuperación completa de los datos.

5

Recuperación eficiente

Minimizar el tiempo de inactividad y garantizar una recuperación rápida tras un incidente de pérdida de datos es vital para mantener las operaciones del negocio.

6

Entornos híbridos

Navegar por las complejidades de los entornos híbridos de TI requiere adaptaciones tanto para entornos en las instalaciones locales como en la nube.

veeam

1. Amenazas para la seguridad

Microsoft Entra ID es parte integral de la estrategia de Identity and Access Management (IAM) en Microsoft 365, Azure y muchas otras plataformas. A menudo desapercibido para los usuarios, su uso es crucial cada vez que inician sesión. Sin embargo, es precisamente esta invisibilidad lo que convierte a Microsoft Entra ID en un objetivo principal para los ciberdelincuentes.

Los actores de amenazas están evolucionando constantemente sus tácticas, y solo necesitan tener éxito una vez, mientras que los defensores deben ser perfectos cada vez. Los atacantes son expertos y emplean tácticas como el phishing y el relleno de credenciales, en las que las contraseñas robadas se utilizan para vulnerar las cuentas. El ransomware, aunque es diferente, es igualmente perjudicial, ya que impide que las organizaciones accedan a sus entornos en la nube y detiene las operaciones.

En un mundo ideal, las organizaciones optarían por evitar que se produzcan infracciones en primer lugar. Muchas estrategias de mitigación de riesgos son muy eficaces, y recursos como la monitorización proactiva y las herramientas de análisis de amenazas son de gran ayuda.

Sin embargo, ninguna defensa es infalible. Aquí es donde el backup y la recuperación se vuelven esenciales. Una estrategia sólida de backup garantiza que, incluso si los atacantes violan sus defensas, pueda restaurar rápidamente el acceso a los datos de identidad críticos. Ya sea para recuperarse del ransomware, revertir borrados accidentales o mitigar amenazas internas, los backups actúan como su red de seguridad.

Para Microsoft Entra ID, redundancia no significa exageración, significa supervivencia. Cuando se realizan backups de los datos de identidad y se pueden recuperar fácilmente, las organizaciones se protegen contra los efectos paralizantes de la pérdida de esos datos.

2. Cumplimiento

El cumplimiento normativo es imprescindible para la mayoría de las empresas, ya que leyes como el RGPD y la HIPAA exigen un estricto cumplimiento de la privacidad, la seguridad y la transparencia de los datos. Hay mucho en juego: el incumplimiento puede resultar en sanciones de hasta el 4% de los ingresos anuales o 20 millones de euros, lo que sea mayor.

En el contexto de Microsoft Entra ID, el cumplimiento depende de la administración adecuada de los permisos de usuario y grupo. Las configuraciones incorrectas o los cambios no autorizados pueden exponer datos confidenciales, lo que lleva a infracciones de cumplimiento. Por ejemplo, si un administrador concede accidentalmente permisos excesivos o elimina un grupo de usuarios críticos, los datos confidenciales podrían caer en las manos equivocadas y los reguladores no dudarán en actuar.

Para cumplir con la normativa, las organizaciones necesitan controles de seguridad sólidos, que incluyan el cifrado, la administración del acceso y el registro de auditoría. Pero una de las herramientas más esenciales en su kit de herramientas de cumplimiento es una solución de backup integral.

Los backups garantizan que los datos de Microsoft Entra ID estén siempre seguros, sean recuperables y cumplan la regulación. Si se produce un error de configuración o un cambio no autorizado, puede detectarlo rápidamente y restaurar la configuración correcta, minimizando el riesgo de incumplimiento y la exposición de datos.

3. Borrados accidentales y errores de configuración

Imagine si un administrador elimina accidentalmente un grupo de usuarios crítico o configura incorrectamente los controles de acceso en Microsoft Entra ID. De repente, los usuarios legítimos no pueden acceder a los sistemas esenciales o, lo que es peor, los usuarios no autorizados obtienen acceso. En un sistema tan central como Microsoft Entra ID, incluso un pequeño error puede tener consecuencias de gran alcance.

Las repercusiones de estos errores de configuración y eliminaciones son profundas. Pueden dejar inaccesibles los sistemas críticos, lo que provoca tiempos de inactividad operativos, pérdidas de productividad y requiere costosos procesos de recuperación. Además, estos errores pueden dañar la confianza que los clientes y socios depositan en una organización, afectando potencialmente las relaciones comerciales a largo plazo.

Pero aquí está la buena noticia: una solución de backup integral puede convertir el desastre en un contratiempo menor. Con los backups, las eliminaciones accidentales o los errores de configuración se pueden corregir en minutos. Tanto si se trata de restaurar un grupo de usuarios eliminado como de volver a una configuración segura previa al error, los backups adecuados garantizan que los errores no se conviertan en una espiral de crisis.

Los errores se producirán; forma parte de la naturaleza humana. Pero con una estrategia sólida de backup, sus consecuencias son más prevenibles que nunca.

4. Limitaciones de la papelera de reciclaje

Además de su breve escala de tiempo de retención, la papelera de reciclaje nativa de Microsoft Entra ID tiene un alcance limitado. Los tipos de datos, como las asignaciones de roles y las directivas de acceso condicional, no se conservan en absoluto, por lo que quedan inmediatamente inaccesibles tras su eliminación, lo que significa que no hay segundas oportunidades. Las restricciones en el volumen de datos recuperables también presentan limitaciones. La papelera de reciclaje de Microsoft Entra ID es una característica útil, pero está lejos de ser una solución completa. Si bien ofrece una ventana de recuperación de hasta 30 días para ciertos tipos de datos, esto se queda corto en escenarios del mundo real. Según el Informe de Defensa de Microsoft 2024, el tiempo medio de detección de incidentes es de 207 días, mucho más allá del periodo de retención de la papelera de reciclaje. Cuando se da cuenta de que faltan datos, a menudo ya es demasiado tarde para recuperarlos.

La historia de la papelera de reciclaje es la siguiente: una vez que expira el período de retención o si los datos omiten la papelera de reciclaje debido a eliminaciones manuales o eliminaciones permanentes, la recuperación mediante las herramientas nativas de Microsoft se vuelve imposible. Una solución de backup dedicada es la única manera de cerrar estas brechas y extenderse más allá de las protecciones integradas de Microsoft. Implementar una solución de backup proporciona una red de seguridad confiable frente a pérdidas de datos accidentales o intencionales y garantiza que casi todos los tipos de datos de identidad sean recuperables.

5. Recuperación eficiente

Las brechas no siempre comienzan con una explosión. Muchas comienzan con pequeños cambios que pasan desapercibidos: un ajuste no autorizado de los permisos, la eliminación de un grupo de seguridad o un pequeño ajuste en la configuración. La capacidad de detectar estos cambios a tiempo es vital para evitar que se conviertan en amenazas graves.

La clave para evitar estos problemas es la detección acelerada de cambios. Los administradores deben ser capaces de anticipar y abordar los problemas antes de que requieran una respuesta importante. Las opciones de recuperación granular permiten a las organizaciones restaurar exactamente los objetos que se necesitan, desde una sola cuenta de usuario hasta una estructura de directorios completa, de manera eficiente y sin provocar tiempos de inactividad innecesarios.

Entonces, ¿cómo se ve la recuperación efectiva para Microsoft Entra ID? Es una combinación de:

- **Comparación de metadatos:** antes de restaurar, compare las configuraciones de producción con los puntos de restauración de backup. Este paso garantiza que identifique exactamente lo que ha cambiado para que pueda restaurar solo lo necesario.
- **Restauración a nivel de objeto:** con las capacidades de restauración granular a nivel de objetos, puede recuperar elementos específicos sin interrumpir el resto de su entorno.
- **Backups periódicos:** asegúrese de que todos los cambios y configuraciones se guardan periódicamente en un repositorio seguro. Esto crea una red de seguridad confiable, lo que permite una restauración rápida y precisa cuando surgen problemas.
- **Planes de recuperación viables:** proporcione procesos claros y paso a paso para restaurar los sistemas, de modo que su organización pueda tener una recuperación rápida, segura y sin problemas.

Juntos, estos elementos forman una estrategia de recuperación completa que minimiza el tiempo de inactividad, reduce el riesgo y mantiene su entorno de Microsoft Entra ID seguro y accesible.

6. Entornos híbridos

La administración de la identidad entre Active Directory (AD) en las instalaciones locales y Microsoft Entra ID en un entorno híbrido aporta flexibilidad y complejidad. Dado que los usuarios se sincronizan constantemente entre los sistemas en la nube y en las instalaciones locales, el borrado accidental, los errores de configuración o los incidentes de sincronización pueden interrumpir el acceso e introducir riesgos de seguridad. Cuando se elimina un usuario, ya sea de forma intencional o por error, la capacidad de restaurar no solo su identidad, sino también sus relaciones y permisos, es crucial para la continuidad del negocio.

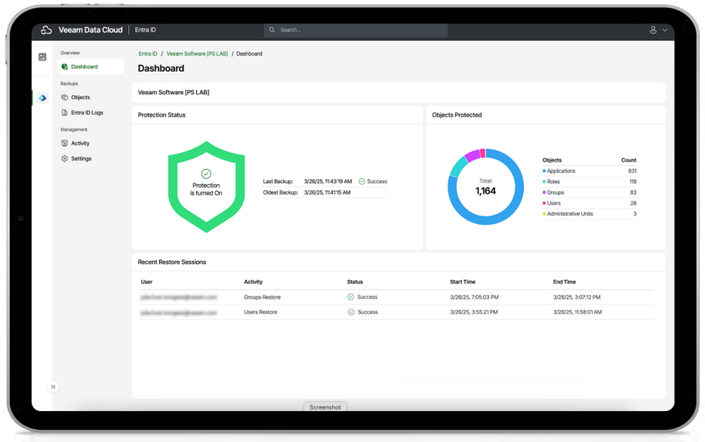
Microsoft Entra Connect y otras herramientas de sincronización se centran en mantener la coherencia de los datos de identidad entre AD y Entra ID, pero no están diseñadas para la recuperación completa. Cuando se elimina un usuario sincronizado, Entra Connect puede restaurarlo sin sus roles, pertenencias a grupos y licencias originales, lo que obliga a los administradores a reconstruir manualmente su identidad. Este proceso lleva mucho tiempo y aumenta el riesgo de restauraciones incompletas o desalineación de privilegios.

La administración de identidades híbridas no se trata solo de mantener a los usuarios activos, sino de restaurarlos con el acceso, los roles y la configuración de seguridad correctos intactos. Sin una estrategia de backup adecuada, los equipos de TI pueden pasar horas arreglando manualmente problemas de acceso tras un borrado o un percance de sincronización.

Veeam Data Cloud for Microsoft Entra ID

Los desafíos de proteger Microsoft Entra ID son claros: los errores humanos, las amenazas cibernéticas y las exigencias de cumplimiento crean riesgos constantes. Sin una estrategia de backup resiliente, incluso un pequeño paso en falso puede conducir a tiempos de inactividad, pérdida de productividad y violaciones de seguridad.

Microsoft Entra ID es la columna vertebral de la identidad digital de su organización y su protección no es negociable. Con **Veeam Data Cloud for Microsoft Entra ID**, puede simplificar la protección de datos y garantizar que su infraestructura de identidad permanezca segura, compatible y siempre disponible.



Esta solución de backup SaaS ofrece:

Backup y restauración integrales: proteja usuarios, grupos, registros de aplicaciones y varios otros objetos

Almacenamiento ilimitado: escale sin esfuerzo con el almacenamiento ilimitado integrado en la solución de backup SaaS

Experiencia de usuario sin problemas: una interfaz de usuario moderna y unificada diseñada para facilitar su uso.

Microsoft Entra ID es demasiado crítico como para dejarlo desprotegido. Los riesgos son reales, pero también lo es la solución. Veeam brinda la seguridad, resiliencia y tranquilidad que las organizaciones modernas necesitan para mantener su infraestructura de identidad protegida, conforme a las normas y siempre disponible.

→ Solicitar una demostración

→ Contactar con equipo de ventas

Más información sobre la protección de Microsoft 365

Haga backup de Microsoft 365 y Entra ID juntos

Este informe le mostrará:

- De qué es responsable su organización en relación a Microsoft 365
- Por qué es tan importante hoy en día proteger los datos de Microsoft 365
- Cómo identificar los vacíos de seguridad en sus organizaciones
- Los beneficios de aprovechar un servicio de backup frente a otros métodos

→ 7 razones críticas para hacer backup de Microsoft 365