eBOOK

PROTEGIENDO LAS

Joyas de la Corona

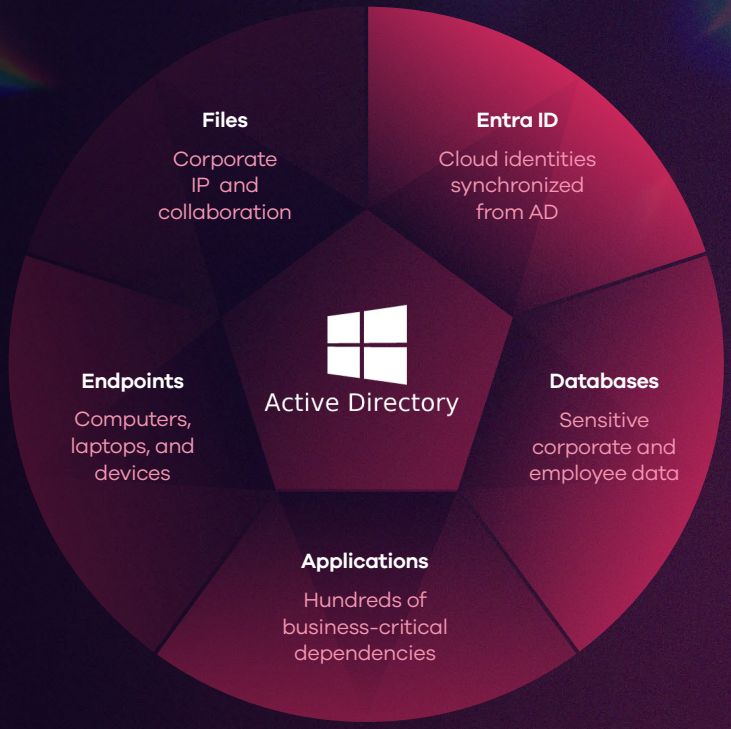
Seguridad de Active Directory contra amenazas cibernéticas

Commvault®

La importancia de Active Directory

Microsoft Active Directory (AD) y Entra ID son las joyas de la corona en la gestión de identidades y acceso empresarial, autenticando millones de usuarios a nivel global y controlando el acceso a sistemas de negocio críticos. Desde los inicios de sesión en estaciones de trabajo hasta el acceso físico a edificios, AD posibilita la operación fluida de cualquier organización.

Si los datos de AD se corrompen o el directorio mismo no está disponible, puede interrumpir gravemente las aplicaciones y procesos de negocio, bloqueando el acceso de los usuarios a sistemas y recursos vitales.



Sin AD, las operaciones comerciales se paralizan.

El personal bancario no puede acceder a las cuentas de los clientes.

Los médicos y enfermeras no pueden acceder a los registros médicos.

Los programadores no pueden publicar código.

Los managers no pueden enviar correos electrónicos.

Los equipos no pueden colaborar ni chatear.

La importancia y complejidad de Active Directory lo hacen un objetivo principal para atacantes

Dado que AD y la gestión de identidades son componentes cruciales de las operaciones empresariales, presentan un objetivo muy atractivo para los atacantes que buscan sistemas valiosos para exigir rescate. Para aquellos que simplemente quieren causar caos, AD es uno de los sistemas que puede paralizar todos los demás y devastar el negocio.

AD es el centro de la autenticación segura y los servicios, y es crucial mantener su seguridad y recuperabilidad, y prepararse para las diversas catástrofes que podrían afectarlo.

AD está involucrado en aproximadamente

9/10

ataques[1]

Esto no es sorprendente, dada la importancia de Active Directory

Los informes de Microsoft Digital Defense indican que el

88%

de los clientes

afectados por incidentes de seguridad tenían una configuración insegura de AD, lo que convierte a AD en un activo de alto valor que los actores malintencionados están ansiosos por explotar[2]

Para los atacantes, AD es un punto de acceso único para elevar privilegios y robar, corromper o negar el acceso a aplicaciones y datos críticos.

Un informe reciente de IBM destaca un aumento del **100%** en los ataques de "kerberoasting",

donde los atacantes intentan obtener privilegios elevados abusando de Microsoft AD[3]

1 Researchers Explore Active Directory Attack Vectors
2 Microsoft Digital Defense Report 2022
3 IBM Report: Identity Comes Under Attack Straining Enterprises' Recovery Time from Breaches

Recuperación de AD: la base del negocio continuo

La importancia de priorizar la recuperación de AD queda evidente cuando se considera su efecto en cascada sobre otras cargas de trabajo. Las aplicaciones, sistemas de archivos, servicios de correo electrónico y bases de datos dependen de AD para una autenticación y acceso de usuario adecuados. Cuando AD se daña o se desconecta por completo, las aplicaciones y servicios críticos se vuelven inaccesibles.

Dado que casi todo en los negocios modernos depende de la identidad, restaurar AD antes de otras cargas de trabajo es una prioridad crítica.

Al restaurar AD primero, las organizaciones pueden reestablecer el control sobre sus redes y sistemas, verificar que las políticas de seguridad de datos y acceso se estén cumpliendo, y proporcionar una base estable para la recuperación de otros sistemas y servicios.

LOS ERRORES OCURREN

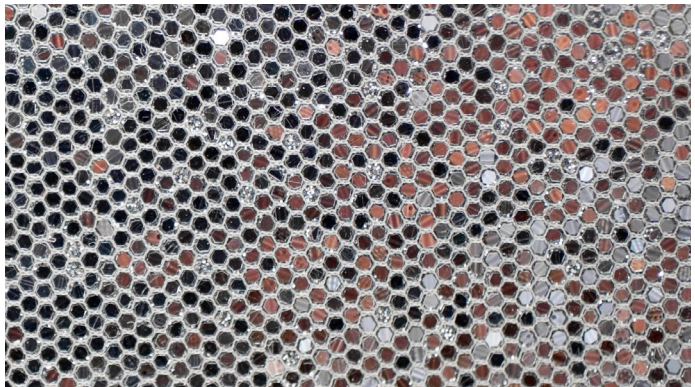
La necesidad de una recuperación granular

Uno de los aspectos más críticos de la protección de AD es la capacidad de restaurar datos perdidos o corruptos rápidamente. Cuando datos importantes dentro de AD se eliminan, cambian o corrompen accidentalmente o de manera maliciosa, es necesario poder identificar rápidamente esos cambios y restaurar y recuperar objetos y atributos individuales.

Aunque es útil que la Papelera de Reciclaje en AD pueda recuperar temporalmente objetos eliminados, depender de este método es arriesgado. La Papelera de Reciclaje solo retiene objetos eliminados durante un tiempo limitado antes de que se eliminen permanentemente. No admite el deshacer cambios a nivel de atributo ni la reversión de modificaciones en Objetos de Política de Grupo (GPO) o configuraciones de AD.

A veces, los desastres pueden no resultar en la eliminación de objetos, sino en la sobre escritura de datos de atributos en múltiples objetos. Por ejemplo, un script de PowerShell mal escrito podría causar cambios inesperados en todo el directorio. Cuando esto ocurre, se necesita la capacidad de localizar y revertir atributos específicos en múltiples objetos dentro de AD. Sin embargo, la Papelera de Reciclaje no puede deshacer cambios a nivel de atributo ni revertir modificaciones a GPOs o configuraciones de AD.

Para una protección completa, es mejor tener una copia de seguridad completa y frecuente de todo AD. Una solución dedicada de protección de datos permite la recuperación granular, restaurando solo el atributo de objeto faltante, dañado o mal configurado. Esta granularidad puede poner rápidamente los sistemas de negocio o los usuarios de nuevo en línea sin necesidad de restaurar todo el entorno de AD.



¿Tienes un plan de recuperación?

Cuando el ransomware bloquea y desconecta los servidores que alojan tu AD, necesitas la capacidad de recuperar el entorno de AD. Esto implica reconstruir el servicio de directorio, incluyendo dominios, controladores de dominio y datos asociados, a un estado previo al ataque.

El impacto de un ataque a AD que deshabilita los controladores de dominio es real y puede ser devastador. Los sistemas críticos dejan de funcionar. Los empleados no pueden iniciar sesión. Las políticas de seguridad que dependen de la identidad no se pueden hacer cumplir.

"Si no podemos recuperar nuestros controladores de dominio, no podemos recuperar nada"

ADMINISTRADOR DE TI, MAERSK

Con amenazas como estas acechando, tener un plan de recuperación bien documentado y frecuentemente probado para reconstruir y restaurar tu entorno de AD a un estado previo y saludable antes del ataque es crucial y la clave para recuperar rápidamente tu negocio.

Ataque de Ransomware

En 2017, el gigante global de transporte marítimo Maersk fue víctima del ciberataque NotPetya, que cifró los sistemas de archivos de

45.000 PC

4.000 servidores

150 controladores de dominio de AD

Con AD completamente fuera de línea, las operaciones se detuvieron inmediatamente, cerrando

17 puertos de envío globales

100s de buques contenedores durante 10 días

En total, el ataque le costó a la empresa al menos

300 millones de dólares

4 The Untold Story of NotPetya, the Most Devastating Cyberattack in History

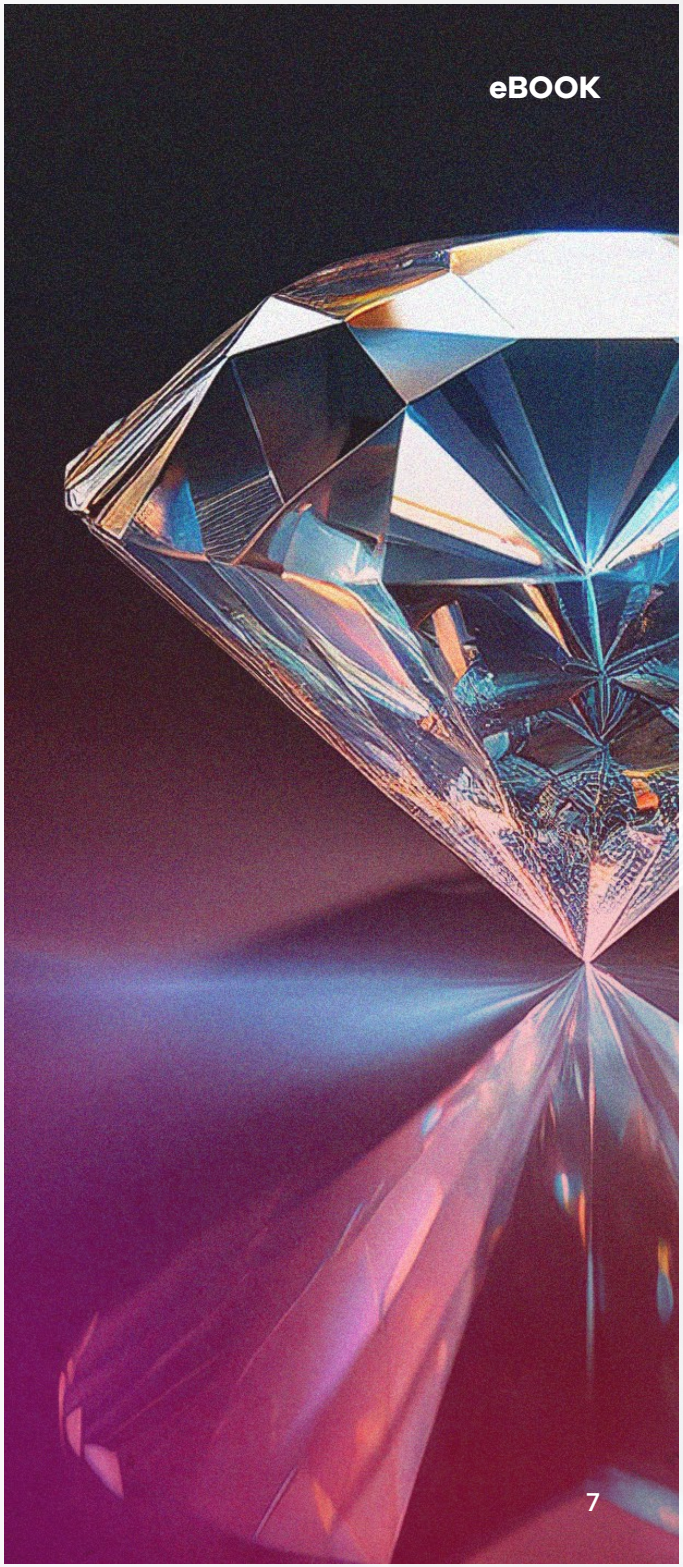
Recuperación de Active Directory: una tarea compleja

Los bosques de AD son entornos complejos con múltiples dominios, varios controladores de dominio para cada uno de esos dominios, y una jerarquía completa de usuarios, ordenadores y configuraciones de acceso y seguridad. En caso de un ciberataque, no es suficiente con restaurar un solo controlador de dominio desde una copia de seguridad. El proceso de recuperación y reconstrucción del entorno es increíblemente intrincado y requiere una coordinación meticulosa. Cada controlador de dominio debe sincronizarse y restaurarse cuidadosamente para evitar inconsistencias de datos y posibles corrupciones.

La Guía de Recuperación de Bosques de AD de Microsoft proporciona un método detallado y paso a paso para esto, que puede implicar desde 50 hasta 100 o más pasos individuales, dependiendo del tamaño de tu organización.

El proceso de recuperación es manual, tedioso y complejo, y completarlo puede llevar de días a semanas. Durante todo este tiempo, las operaciones comerciales dejan de funcionar y los usuarios no pueden acceder a aplicaciones importantes.

Sin automatizar y orquestar el proceso, se corre el riesgo de restaurar AD a un estado no utilizable, lo que podría interrumpir aún más el negocio y prolongar la interrupción.



Commvault hace que tu Active Directory sea resiliente

Commvault Cloud Backup & Recovery for Active Directory te permite proteger y acelerar la recuperación de datos de AD ante la corrupción, la eliminación accidental y los ataques de ransomware.

Acelera la recuperación de AD y vuelve a la normalidad más rápidamente con:

Recuperación de bosques automatizada:

Recupera rápidamente los bosques a un punto en el tiempo antes del ataque, permitiéndote volver a la normalidad en horas en lugar de días o semanas.

Comparaciones interactivas:

Identifica cambios en el dominio, lo que te permite recuperar rápidamente objetos eliminados por error o de manera maliciosa, o revertir atributos sobrescritos en el directorio.

Recuperación flexible y granular:

Recupera rápidamente solo los atributos de objeto desaparecidos, dañados o mal configurados, y pon a tus sistemas de negocio o usuarios de nuevo online de manera rápida.

Soporte para directorios híbridos:

Protege objetos críticos de Microsoft AD y Entra ID, incluyendo GPOs, usuarios, grupos, políticas de acceso condicional, roles y más.

Pruebas de recuperación de AD:

Proporciona confianza en que las recuperaciones pueden ser exitosas y permite que los equipos de seguridad y TI se preparen en tiempos buenos para estar listos en tiempos malos.

La recuperación cibernética es más que solo AD

Enfrentarse a un ciberataque o a una situación de ransomware es una experiencia aterradora.

Restaurar AD es el primer paso en la mayoría de los casos, y encontrar formas de automatizar un proceso que, de otro modo sería intensivo en tiempo y recursos, puede ayudar a impulsar el proceso de recuperación y devolver rápidamente el negocio a la normalidad. Aún mejor es cuando tu recuperación de AD se basa en la misma plataforma en la que se apoya el resto de tu recuperación cibernética.

Unificar el proceso de recuperación y reconstrucción cibernética en una plataforma común permite una coordinación, automatización y orquestación fáciles que abarcan más que solo la recuperación de identidades. Puedes orquestar la recuperación de aplicaciones, datos, nubes e infraestructura. Esto ayudará a que tus equipos trabajen juntos para reconstruir tus sistemas después de ciberataques y desastres, y construir una resiliencia que garantice la continuidad del negocio.

eBOOK

Solicita una Demo y descubre como puedes restarurar tu bosque de AD completo con solo unos clics para mantener tu negocio continuo.

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®