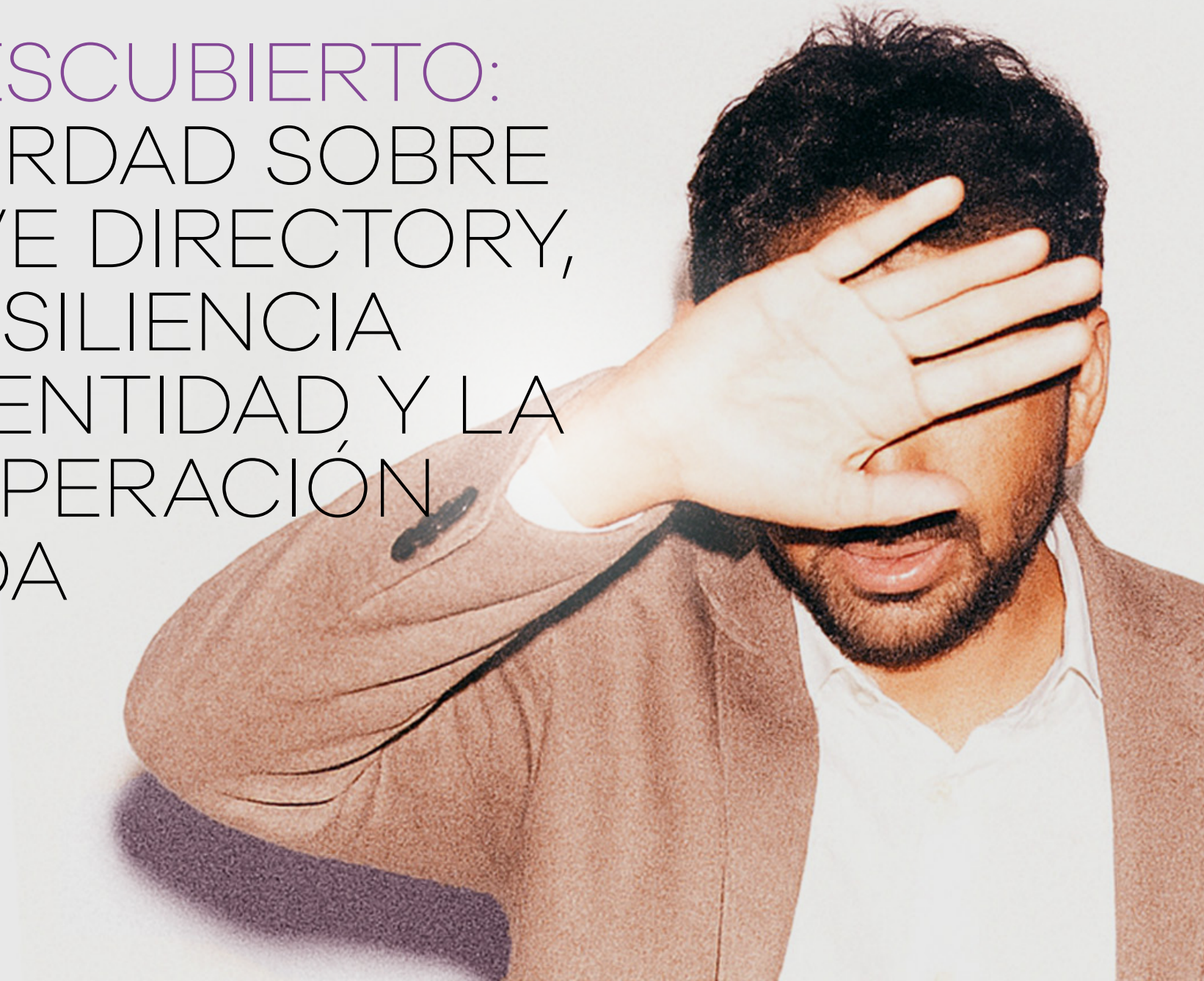
eBOOK

AL DESCUBIERTO: LA VERDAD SOBRE ACTIVE DIRECTORY, LA RESILIENCIA DE IDENTIDAD Y LA RECUPERACIÓN RÁPIDA



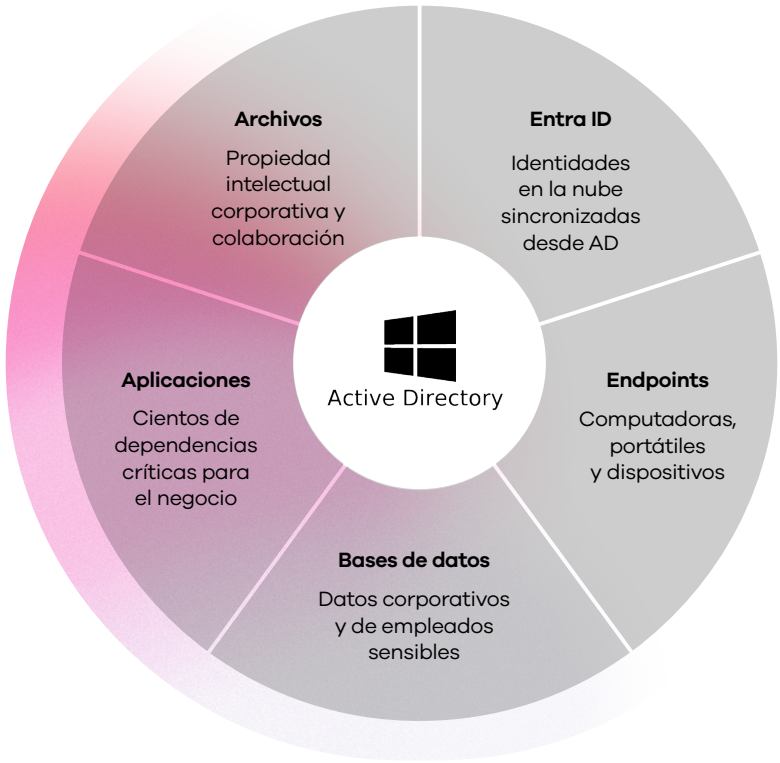
Commvault®

LA DURA REALIDAD ES ESTA: LA INFRAESTRUCTURA DE IDENTIDAD DIGITAL DE TU ORGANIZACIÓN ESTÁ BAJO ASEDIO

Microsoft Active Directory (AD) y Entra ID son las joyas de la corona de la gestión de identidad y acceso empresarial, ya que autentican a millones de usuarios en todo el mundo y controlan el acceso a sistemas críticos de negocio. Desde inicios de sesión en estaciones de trabajo hasta el acceso físico a edificios, AD permiteelfuncionamiento sin interrupciones de tu organización, convirtiéndose en el objetivo principal para los ciberdelincuentes.

Pero hay algo que la mayoría de las organizaciones no se da cuenta: los enfoques tradicionales de backup y recuperación para AD son, en esencia, inadecuados en el panorama actual de amenazas. La verdad sobre la resiliencia de identidad va mucho más allá de la simple protección de datos: requiere una estrategia integral que anticipe ataques sofisticados y habilite una recuperación rápida y automatizada a la velocidad que exige el negocio.

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



SIN AD, LAS OPERACIONES DE NEGOCIO SE DETIENEN POR COMPLETO.

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

Los médicos y enfermeras **no pueden acceder a los historiales médicos.**

Los programadores y desarrolladores **no pueden publicar código.**

Los gerentes **no pueden enviar correos electrónicos.**

Los equipos **no pueden colaborar ni chatear.**

AL DESCUBIERTO: Por qué 9 de cada 10 ataques tienen como objetivo su infraestructura de identidad

La realidad de la ciber-guerra moderna es que la infraestructura de identidad se ha convertido en el principal campo de batalla. Dado que AD y la gestión de identidades son componentes tan cruciales para las operaciones empresariales, representan un objetivo muy atractivo para los atacantes que buscan sistemas valiosos para retener como rehenes. Para aquellos que simplemente desean causar caos, AD es uno de los sistemas que puede detener a todos los demás y devastar el negocio.

Aquí es donde la resiliencia de identidad se vuelve crítica. La resiliencia de identidad no se trata solo de hacer copias de seguridad de su directorio: se trata de construir una infraestructura de identidad que pueda resistir, adaptarse y recuperarse rápidamente de ataques sofisticados mientras se mantiene la continuidad del negocio.

AD es el centro de la autenticación y los servicios seguros, y es fundamental mantener su seguridad y capacidad de recuperación, preparándose para los diversos desastres que podrían afectarlo.

Las estadísticas dibujan un panorama sombrío del escenario de amenazas actual.

AD está involucrado en aproximadamente

9 de cada 10

ataques.

Esto no es sorprendente, dada la importancia de AD.

Microsoft Digital Defense informa que el

88%

de los clientes

afectados por incidentes de seguridad tenían una **configuración de AD insegura**, lo que convierte AD en un activo de alto valor para los atacantes malintencionados.

Para los atacantes, AD es una ventanilla única para escalar privilegios, 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".**

Aquí es donde los atacantes intentan obtener privilegios elevados abusando de Microsoft AD.

LA DEPENDENCIA OCULTA:POR QUÉ TODO CUANDO LA IDENTIDAD CAE

Esto es lo que convierte la recuperación de AD en la base de la continuidad del negocio.

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

La resiliencia de identidad reconoce esta dependencia fundamental.

Dado que casi todo en los negocios modernos depende de la identidad, construir una infraestructura de identidad resiliente se convierte en la piedra angular de la resiliencia organizacional. Esto va mucho más allá de simplemente restaurar AD después de que ocurre un ataque.

Al establecer prácticas de resiliencia de identidad, las organizaciones pueden mantener un mejor control sobre sus redes y sistemas incluso durante ataques activos, hacer cumplir las políticas de seguridad de datos y acceso, y proporcionar una base estable que respalde la recuperación rápida de otros sistemas y servicios.

AL DESCUBIERTO: LA DEFECTO FATAL EN LAS HERRAMIENTAS RECUPERACIÓN INTEGRADAS DE AD

Uno de los aspectos más críticos de la protección de AD es la capacidad de restaurar rápidamente los datos perdidos o dañados. Cuando los datos importantes dentro de AD se eliminan, modifican o corrompen accidental o maliciosamente, es necesario poder identificar rápidamente esos cambios y restaurar y recuperar objetos y atributos individuales.

La incómoda verdad sobre las opciones de recuperación integradas de AD: Aunque es útil que la Papelera de reciclaje en AD pueda recuperar temporalmente objetos eliminados, confiar en este método es arriesgado. La Papelera de reciclaje solo retiene los objetos eliminados por un tiempo limitado antes de que se eliminen de forma permanente. No admite revertir cambios a nivel de atributos ni deshacer modificaciones en Objetos de Directiva de Grupo (GPOs) o configuraciones de AD.

A veces, los desastres no resultan en la eliminación de objetos, sino en la sobrescritura 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 atributos ni revertir modificaciones a GPOs o configuraciones de AD.

La verdadera resiliencia de identidad exige capacidades de recuperación granular. Para una protección integral, lo mejor es contar con una copia de seguridad completa y frecuente de todo AD que admita operaciones de recuperación precisas a nivel de objeto.

Una solución de protección de datos dedicada permite una recuperación granular, restaurando únicamente el atributo de objeto que falta, está dañado o mal configurado. Esta granularidad puede devolver rápidamente los sistemas empresariales o a los usuarios online sin necesidad de una restauración completa de todo el entorno de AD.

Cuando golpea el ransomware, ¿tienes un plan para una recuperación rápida?

Cuando el ransomware bloquea y deja fuera de línea los servidores que alojan su AD, necesitas la capacidad de recuperar el entorno de AD. Esto implica reconstruir el servicio de directorio, incluidos los dominios, controladores de dominio y los 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 aplicar.

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

ADMINISTRADOR DE TI, MAERSK

Este estudio de caso revela la importancia crítica de contar con capacidades de recuperación rápida dentro de una estrategia de resiliencia de identidad. Con amenazas como estas, tener un plan de recuperación bien documentado y probado con frecuencia para reconstruir y restaurar su entorno de AD a un estado saludable previo al ataque es fundamental y la clave para que tu negocio vuelva a funcionar.

LA LECCIÓN DE $300 MILLONES: LO QUE EL DESASTRE DE MAERSK REVELA SOBRE LA RECUPERACIÓN

En 2017, el gigante naviero global Maersk fue víctima del ciberataque NotPetya, que encriptó los sistemas de archivos de:

45K PCs

4K servidores

149/150 controladores de dominio de AD

Con AD fuera de línea, las operaciones cesaron instantáneamente, deteniendo:

17 puertos marítimos globales

100s de buques portacontenedores, varados durante **10 días**

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

$300M

AL DESCUBIERTO: EL PROCESO DE RECUPERACIÓN DE 100 PASOS QUE ESTÁ DESTINADO A FALLAR

La realidad de la complejidad de la recuperación de AD: 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, computadoras y configuraciones de acceso/seguridad. En el caso de un ciberataque, no basta 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 una posible corrupción.

La Guía de Recuperación de Bosques de AD de Microsoft ofrece un método detallado paso a paso para este proceso, que puede implicar entre 50 y 100 o más pasos individuales, según el tamaño de su organización.

La dura realidad de la recuperación manual: El proceso de recuperación es manual, consume mucho tiempo, es complejo y propenso a errores, a menudo tomando días o incluso semanas en completarse. Durante todo este tiempo, las operaciones de negocio dejan de funcionar y los usuarios no pueden acceder a aplicaciones importantes. Este tiempo de inactividad prolongado contradice directamente los principios de la resiliencia de identidad, que exige capacidades de restauración rápida.

Sin automatizar ni orquestar el proceso, corres el riesgo de restaurar AD a un estado inutilizable, lo que podría interrumpir aún más el negocio y prolongar una interrupción.

LA SOLUCIÓN: CÓMO DISEÑAR UNA RESILIENCIA DE IDENTIDAD SÓLIDA CON COMMVAULT

La solución para crear resiliencia de identidad: Commvault Cloud Backup & Recovery para Active Directory te permite proteger y acelerar la recuperación de los datos de AD frente a la corrupción, la eliminación accidental y los ataques de ransomware.

Acelera la recuperación de AD y diseña resiliencia de identidad, volviendo al negocio más rápido con:

Recuperación automatizada de bosques de AD

Restaura bosques rápidamente a un punto en el tiempo antes de un ataque, permitiéndote volver al negocio en horas en lugar de días o semanas.

Comparaciones interactivas

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

Recuperación flexible y granular

Restaura rápidamente solo los atributos de objetos que estén faltantes, dañados o mal configurados, y devuelve los sistemas empresariales o usuarios online rápidamente.

Soporte de directorio híbrido

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

Pruebas de recuperación de AD

Brinda confianza en que las recuperaciones pueden tener éxito y permite que los equipos de seguridad y TI practiquen en tiempos de calma para estar preparados ante tiempos difíciles.

MÁS ALLÁ DE LA IDENTIDAD: LA ESTRATEGIA COMPLETA DE CIBERRECUPERACIÓN

La ciberrecuperación es más que solo AD

Enfrentarse a un ciberataque o a una situación de ransomware es una experiencia angustiante. Restaurar AD es el primer paso en la mayoría de los casos, y encontrar formas de automatizar el proceso —que de otro modo es intensivo en tiempo y recursos— puede ayudar a acelerar la recuperación y devolver el negocio a la normalidad rápidamente. Aún mejor es cuando la recuperación de AD se construye sobre la misma plataforma en la que se apoya el resto de su estrategia de ciberrecuperación.

La verdadera resiliencia de identidad va más allá de la protección de AD: se integra fácilmente con tu estrategia más amplia de ciberrecuperación. Unificar el proceso de recuperación y reconstrucción cibernética en una plataforma común permite una coordinación, automatización y orquestación sencillas que abarcan más que solo la recuperación de identidad: puedes orquestar la recuperación de aplicaciones, datos, nubes e infraestructura. Esto ayudará a que tus equipos trabajen juntos para reconstruir los sistemas tras ciberataques y desastres, y para construir una resiliencia que garantice la continuidad del negocio.

Solicita una demo y descubre cómo puedes restaurar todo tu bosque de AD en solo unos pocos clics para ayudar a mantener la continuidad del negocio.

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



Commvault®