COMMVAULT

HOJA DE DATOS

Más que protección de datos: backups inmutables en la nube con Commvault

Las ciberamenazas están aumentando rápidamente en sofisticación y persistencia. Y, mientras aumentan las ciberamenazas, expertos como IDC vaticinan que los gastos de seguridad alcancen 133.800 millones de dólares anuales en todo el mundo en 2022[1]. A pesar del aumento en la concienciación y en el gasto, cada 14 segundos una organización será víctima del ransomware, según el Informe Anual sobre Cibercrimen de la publicación especializada CPO Magazine[2]. Estas estadísticas ratifican la importancia de estar preparado para la recuperación. Con el almacenamiento en la nube como opción cada vez más extendida para los backups remotos, la seguridad de los datos se convierte en un apartado crítico. Para abordar esto, muchas soluciones de protección de datos ofrecen robustas opciones WORM y de inmutabilidad para una mayor protección y seguridad en la nube.

Combinando los controles de seguridad líderes de Commvault™ Complete Backup & Recovery con la integración de WORM y almacenamiento inmutable en la nube, las organizaciones podrán estar seguras de que sus datos críticos no podrán ser eliminados, modificados ni leídos por ataques maliciosos externos o internos, manteniendo así el cumplimiento de la normativa vigente.

Controles de seguridad AAA

Commvault protege el acceso, la privacidad y el control de datos de backup residentes en diferentes copias, incluyendo la nube. Los datos de backup inmutable de Commvault utilizan un amplio conjunto de prestaciones e incorporan los principios del marco de seguridad AAA.

Marco de seguridad AAA para el control de accesos

Autenticación	Autorización	Contabilidad
Verificación y concesión de acceso	Control del nivel de acceso requerido	Seguimiento y auditoría de acceso y capacidades

Los controles de **autenticación** proporcionan y otorgan acceso a los datos de backup. Es algo así como un "*gate keeper*". Las características incluyen autenticación certificada, autenticación de dos factores (2FA) e integración con múltiples sistemas de gestión de identidades de terceros con protocolos seguros como LDAPS, SAML y OpenID.

Los controles de **autorización** determinan qué nivel de acceso está permitido en Commvault CommCell. Una vez permitida la autenticación, Commvault incluye controles como seguridad basada en roles, *multi-tenancy*, bloqueos de privacidad y autenticación multi-nivel. Todas estas funciones operan en conjunto para evitar que se acceda a los datos, o que sean retenidos o eliminados. Añadir estas "puertas" facilita el aislamiento del software, e incluso los administradores tienen bloqueada la opción de eliminar o acceder a los datos de backup, o para revertir los controles de seguridad. Del mismo modo, si un actor malicioso obtiene acceso al CommCell de manera ilícita, los datos de backup estarán protegidos ante actividades maliciosas dentro de la plataforma de Commvault.

1 El gasto en soluciones de seguridad en todo el mundo podría alcanzará 103.100 millones de dólares en 2019, según un estudio de IDC. 20 de marzo de 2019

2 CPO Magazine, Undécima edición del informe '*11 Eye Opening Cyber Security Statistics for 2019*', por Matt Powell, 25 de junio de 2019

Por último, Commvault aplica **contabilidad** mediante la auditoría de eventos y acciones dentro de CommCell y proporciona una rica interfaz personalizable para visualizar esta información. Hay cientos de informes fácilmente accesibles a través de la consola central de Commvault que aportan información detallada sobre operaciones, eventos y acciones en CommCell. La información contenida en los informes y los paneles de control solo es visible para usuarios a los que se ha otorgado acceso. Esto permite a los responsables de los datos visualizar los mismos informes y paneles de auditoría que los administradores, pero no podrán ver aquellos recursos para los que no tienen permiso, mientras que la capacidad de personalizar y crear informes utilizando fuentes de datos de Commvault y APIs externas les será útil para ampliar sus capacidades. Para una monitorización continua, Commvault se integra con herramientas de terceros como Syslog, Splunk o SNMP, lo que amplía aún más las capacidades de *acounting* y auditoría dentro de Commvault y proporciona flexibilidad para integrarse con cualquier sistema existente dentro de la organización.

Backups inmutables en la nube

Commvault Complete™ Backup & Recovery proporciona inmutabilidad para el backup local combinando controles de seguridad dentro del marco AAA, fortificación, cifrado de datos y bloqueo nativo de protección ante ransomware. Pero, a la hora de diseñar una solución de protección contra el ransomware y las ciberamenazas, es imprescindible realizar backups fuera de las instalaciones. El almacenamiento en la nube es una solución económica porque los recursos son fácilmente accesibles, elásticos y multi-nivel.

Cuando se utiliza almacenamiento en la nube (por ejemplo, Amazon Web Services o Microsoft Azure), se habilitan opciones de inmutabilidad en el nivel de almacenamiento de nube. El destino en la nube se configura como una librería dentro de Commvault para backup secundario y/o terciario. Cuando se habilita la inmutabilidad en la nube, todo el contenedor de almacenamiento queda bloqueado y los contenidos dentro del contenedor no podrán ser modificados ni eliminados durante el período de inmutabilidad predefinido.

Utilizar Commvault con almacenamiento inmutable en la nube ofrece ventajas clave en comparación con otros productos de backup:

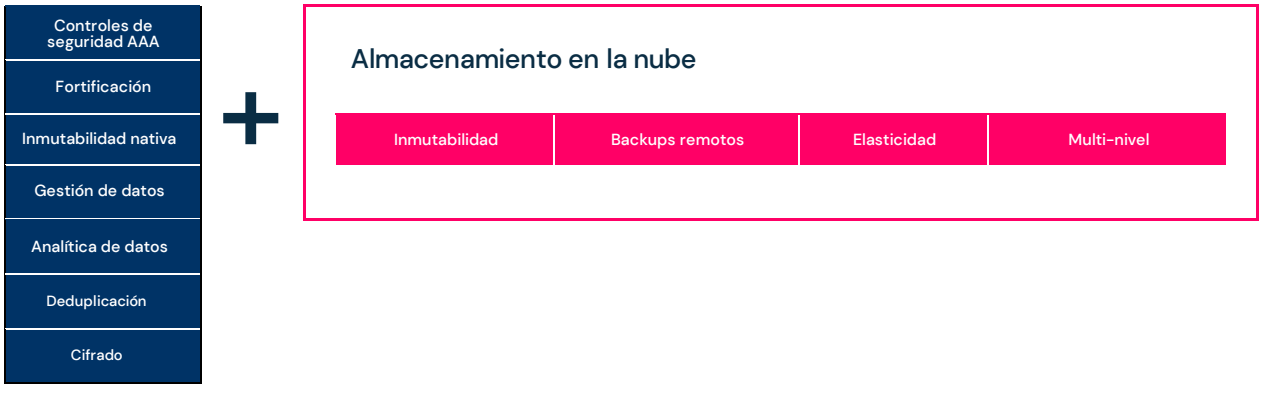
Controles de seguridad y fortificación con Commvault

Si un actor malicioso consigue tus credenciales en la nube, le será imposible eliminar, cifrar, manipular o revertir las opciones de inmutabilidad aplicadas a los datos de backup. Los controles de seguridad AAA y las capacidades de fortificación (*hardening*) de Commvault actúan como primera línea de defensa, evitando que el actor malicioso obtenga acceso a los datos o los elimine, mientras que el bloqueo inmutable en el almacenamiento proporcionará una segunda capa de protección para los datos de backup.

Deduplicación

Cuando las organizaciones tienen que enviar múltiples *Petabytes* de datos a la nube, el coste y el ancho de banda son esenciales. La deduplicación del software de Commvault comienza donde residen los datos de origen. Solo los bloques modificados se envían a la nube, lo que reduce drásticamente el ancho de banda requerido para las operaciones de copia. Esto, además, permite proteger un mayor número de ciclos de backup en la nube (completos o incrementales), al tiempo que reduce la huella de almacenamiento. En última instancia, la deduplicación de Commvault ayuda a los backups a llegar rápidamente a la nube, así como a reducir los objetivos de punto de recuperación (RPO), incrementar la preparación para la recuperación y minimizar los costes de almacenamiento.

Plataforma de Commvault



Cifrado y gestión de claves

El cifrado del almacenamiento en la nube es perfecto para evitar que los datos en reposo puedan ser utilizados en caso de robo, pero no atiende las necesidades de cifrado en origen. El módulo de cifrado certificado FIPS 140-2 de Commvault se ocupa del cifrado en origen antes de enviar los datos a la nube, lo que garantiza que cada bloque de datos transmitidos estará cifrado y protegido en todo momento. Para niveles de seguridad más profundos, las claves de cifrado se pueden descargar en servidores externos de gestión de claves, incluyendo AWS, Azure o cualquier sistema compatible con KMIP.

Gestión y analítica de datos

Commvault gestiona las políticas de retención y backup, mientras que en la nube se gestionan los bloqueos inmutables configurados en la capa de almacenamiento. Utilizando un enfoque multi-nivel para almacenar datos en la nube, las organizaciones pueden aprovechar opciones de almacenamiento en frío para ahorrar costes, mientras que el índice se conserva disponible en todo momento en las instalaciones o en niveles de almacenamiento en la nube más calientes para propósitos de analítica. Commvault permite que los backups inmutables que existen en el almacenamiento en frío se analicen de una forma rentable y puedan ser aprovechados para otros fines de negocio. Sin la capacidad de utilizar este enfoque de almacenamiento por niveles, los backups en frío serían muy costosos de indexar y analizar debido a los perfiles de acceso impuestos por los proveedores de nube.

Cumplimiento normativo

El uso de WORM en la nube y las opciones de almacenamiento inmutable de Commvault ayudan a las organizaciones a abordar marcos legislativos como SEC 17a-4 (f), CFTC 1.31 (d), FINRA u otras normas relacionadas con la grabación, almacenamiento y retención de registros electrónicos. Commvault soporta las opciones compatibles de almacenamiento de AWS[3] y Azure[4], diseñadas para cumplir con los requisitos de seguridad de la industria, preservando los registros en un formato no regrabable y no borrable con sus respectivas tecnologías de bloqueo de almacenamiento.

Conclusión

Si bien las ciberamenazas siguen aumentando, tu organización puede mantener el ritmo y mitigar los riesgos. Con un almacenamiento en la nube de alta disponibilidad y una mayor protección, te será fácil crear backups secundarios y terciarios en la nube. Sin ningún coste adicional, Commvault Complete Backup & Recovery gestiona, analiza y protege tus datos de backup de manera eficiente, mientras que la inmutabilidad en la nube te permite blindar aún más tus datos ante las ciberamenazas, tanto hoy como en el futuro. Con Commvault tendrás la seguridad y la protección necesarias para almacenar y gestionar tus datos tanto en instalaciones propias como en la nube. Estarás preparado para la recuperación.

3 Evaluación de conformidad para Amazon Glacier con Vault Lock: SEC 17a-4(f) y CFTC 1.31(b)-(c)
4 Evaluación de conformidad para Microsoft Azure Storage: SEC 17a-4(f) y CFTC 1.31(c)-(d)