Refuerce su plan de protección de datos con una solución de ciberrecuperación más sólida y de acción rápida

Según nuestra investigación, Dell Technologies PowerProtect Cyber Recovery puede ofrecer aislamiento físico para vaults de copia de seguridad y un análisis más profundo para detectar ransomware.

Aislamiento de cámara de aire física para vaults de copia de seguridad

Cree una barrera física que los datos no pueden atravesar.

Análisis más profundo para detectar ransomware

CyberSense analiza el contenido de archivos y bases de datos, no solo los metadatos.

Análisis de 2 veces más cargas de trabajo anómalas

Busque malware en más lugares con una sola herramienta.

El coste medio de un ataque de ransomware aumentó casi un 20 % en dos años hasta alcanzar los 5,23 millones de dólares.[1] Las soluciones eficientes de ciberrecuperación pueden ayudar a reducir o incluso evitar estos posibles costes, ya que permiten a las organizaciones recuperarse rápidamente de los incidentes, reducir la pérdida de datos, minimizar el tiempo de inactividad y, en el proceso, preservar la integridad de su marca. Las soluciones deben identificar y restaurar los datos correctos conocidos después del ataque, lo que garantiza que la organización pueda salvar los datos críticos y los sistemas y, al mismo tiempo, ayudar a minimizar los riesgos empresariales y el tiempo de inactividad.

Dell PowerProtect Cyber Recovery (Cyber Recovery) es una solución de este tipo. Ayuda a las organizaciones a proteger sus datos y aplicaciones contra ransomware, ciberataques destructivos y eventos inesperados. Este informe utiliza datos disponibles públicamente para contrastar las características y funcionalidades de protección de datos fundamentales de Cyber Recovery y una solución de la competencia, Rubrik Security Cloud (RSC). Analizamos específicamente las características y la funcionalidad que a los clientes de ciberrecuperación les podrían parecer importantes, como el vault de recuperación, la inmutabilidad, la admisión de cargas de trabajo, la tecnología de análisis, la capacidad de recuperación y el aislamiento.

A diferencia de RSC, Cyber Recovery utiliza un enfoque de varias copias, lo que significa que, después de crear copias de seguridad, las copia (o, normalmente, un subconjunto seleccionado) en un almacenamiento aislado para su protección y análisis. Cyber Recovery consta de varios componentes, incluidos uno o más vaults de almacenamiento, ubicados en las instalaciones en un dispositivo PowerProtect Data Domain o en la cloud a través de Dell APEX Protection Storage for Public Cloud definido por software. En comparación, RSC no ofrece opciones de vault local. Cyber Recovery también incluye CyberSense, un motor de análisis de seguridad inteligente totalmente automatizado e integrado que analiza datos, archivos, bases de datos e imágenes en el vault en busca de signos de daños de un ataque de ransomware. La solución CyberSense puede analizar dos veces más cargas de trabajo anómalas que la solución Rubrik, lo que podría permitir que el ML (aprendizaje automático) de análisis de CyberSense detecte el impacto de malware u otra actividad de atacantes en más datos. Analizaremos cómo PowerProtect Cyber Recovery funciona de manera diferente y podría ser más ventajoso para su organización.

Descripción general del producto

Descripción general de Dell PowerProtect Cyber Recovery

Dell PowerProtect Cyber Recovery consta de un dispositivo de almacenamiento que alberga los datos de producción y un dispositivo de almacenamiento de destino en el vault para la replicación. También incluye el software Cyber Recovery, que coordina la sincronización, gestiona varias copias de datos en el sistema PowerProtect Data Domain (PPDD) en el vault de Cyber Recovery, supervisa el proceso de recuperación
y supervisa el proceso de análisis con CyberSense.

La solución transfiere datos únicos desde el PPDD MTree de producción a su homólogo en el vault a través de la replicación MTree y permite la inmutabilidad de los datos* durante un periodo de tiempo determinado. El vault cuenta con un servidor que contiene el software Cyber Recovery y un componente en el que la solución restaura las aplicaciones y los datos de copia de seguridad. Cada vault de Cyber Recovery suele albergar muchos de estos componentes. El vault también contiene un host de análisis/indexación equipado con software de análisis de datos, que proporciona una integración directa entre el software Cyber Recovery y CyberSense.

*Los productos Dell se han diseñado para ayudar a los clientes en sus esfuerzos por proteger los datos críticos. Igual que en el caso de cualquier producto electrónico, los productos de protección de datos y de almacenamiento, y otros productos de infraestructura pueden sufrir vulneraciones de seguridad. Es importante que los clientes instalen las actualizaciones de seguridad tan pronto como Dell las haga públicas.

En la Figura 1 se ofrece una descripción general de la solución Dell Cyber Recovery.

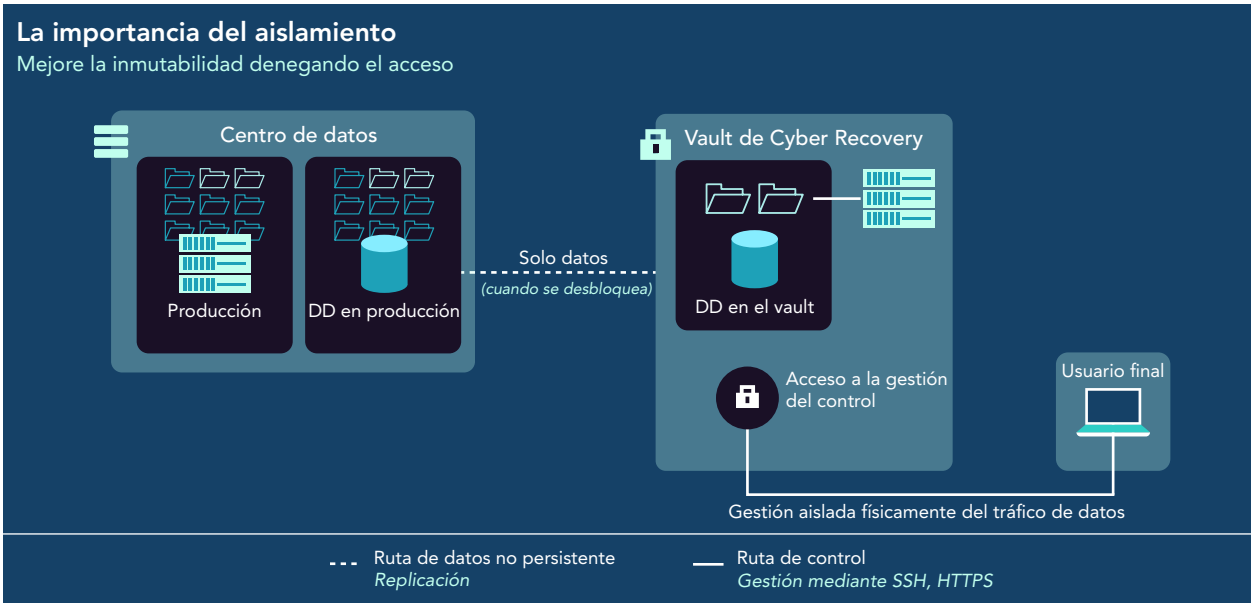

Figura 1: Arquitectura de ruta de control y datos de alto nivel del vault de Cyber Recovery. Fuente: Principled Technologies.

Para obtener más información sobre los componentes clave de la solución Dell PowerProtect Cyber Recovery, lea la Dell PowerProtect Cyber Recovery Solution Guide.

Descripción general de Rubrik Security Cloud

Rubrik describe Rubrik Security Cloud como una plataforma de software como servicio (SaaS) que permite a los clientes "mantener [sus] datos seguros, supervisar el riesgo de los datos y recuperar rápidamente [sus] datos, dondequiera que residan, en la empresa, en la cloud y en las aplicaciones SaaS".[4] Rubrik afirma que creó la solución sobre una "arquitectura de microservicios segura con servicios e infraestructura de alta disponibilidad que se ejecuta en Google Cloud Platform (GCP)".[5] En la Figura 2 se muestra la estructura general de Rubrik Security Cloud.

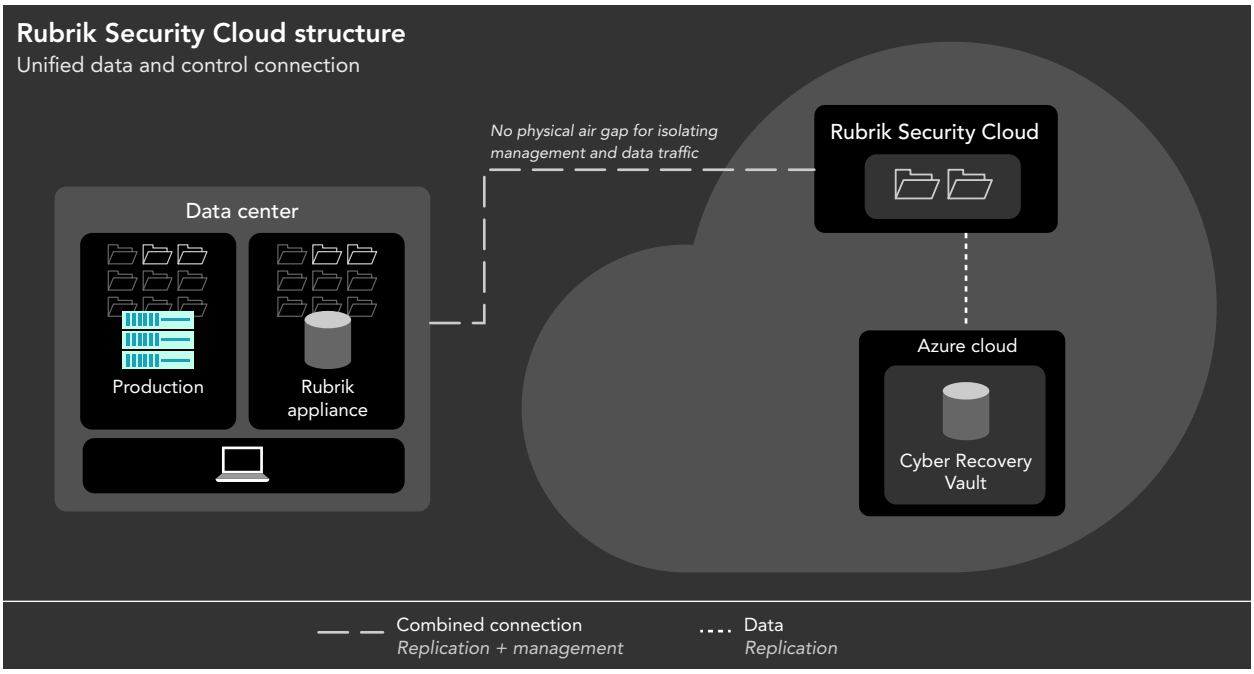

Figura 2: La estructura general de Rubrik Security Cloud. Fuente: Principled Technologies.

Compatibilidad con funciones

Vault de recuperación

Los vaults son el almacenamiento específico que alberga copias cifradas de las copias de seguridad que la solución toma en el entorno de producción. Los vaults no forman parte de las soluciones de copia de seguridad de producción, sino que cada uno sirve a modo de ubicación aislada de "copia de seguridad para la copia de seguridad" a partir de la cual los clientes pueden recuperar copias de seguridad validadas.

Dell ofrece varias opciones de almacenamiento seguro, como en las instalaciones, en un sitio de housing remoto o en una cloud pública. El vault en las instalaciones aprovecha un PPDD operativo aislado que se aloja en su centro de datos, incluso en el mismo rack que la solución de copia de seguridad. Por regla general, una solución aislada se aísla físicamente del entorno de producción. Un vault coubicado fuera de las instalaciones requiere conexiones de red específicas a un vault físico, como una versión en las instalaciones, pero el vault está geográficamente separado en un centro de datos remoto. Dell también proporciona vaults en la cloud pública, colaborando con los proveedores de servicios de cloud Amazon Web Services (AWS), Microsoft Azure y Google Cloud. Los vaults de cloud pública podrían ofrecer flexibilidad de configuración para satisfacer las necesidades de los clientes.[6, 7, 8]

Rubrik Cyber Recovery es un componente de Rubrik Security Cloud. El vault de recuperación, que se proporciona a través de un modelo de software como servicio, solo utiliza almacenamiento en Microsoft Azure. Muchos de los documentos públicamente disponibles que encontramos en nuestra investigación vinculan el Rubrik Cyber Recovery Vault al Rubrik Cloud Vault, el nivel de copia de seguridad, que ofrece inmutabilidad.[9, 10] Este vault no requiere hardware adicional y lo puede utilizar cualquier versión de la plataforma Rubrik Cloud Data Management (CDM) a partir de la versión 6.02.

Inmutabilidad

La inmutabilidad se refiere a la condición de ser inalterable o permanente. Las copias de seguridad inmutables y las copias de seguridad permiten a los administradores crear permanencia para los archivos que los usuarios o sistemas no pueden modificar o eliminar hasta que se haya superado un plazo asignado. A continuación, los archivos se "descargan": la solución los elimina automáticamente. Las soluciones suelen llevar a cabo este proceso mediante políticas o definiciones que rigen la forma en que el sistema trata los archivos.[11]

La inmutabilidad de Dell PowerProtect Cyber Recovery se basa en los bloqueos de retención, a través de la función de bloqueo de retención, para evitar la eliminación o modificación (durante un periodo de tiempo) o el vencimiento anticipado forzado de las copias de seguridad. (El PPDD es un sistema de archivos de solo anexión, con independencia de si la organización ha activado el bloqueo de retención o no[12]). Los clientes de Dell gestionan las copias de seguridad mediante PPDD MTrees, que son particiones lógicas definidas por el usuario con ajustes de retención independientes que asignan como destinos de aplicaciones de copia de seguridad.[13] Los clientes pueden elegir entre dos tipos de bloqueos de retención: gobernanza y cumplimiento normativo. Los bloqueos de cumplimiento normativo son los más estrictos y seguros de los dos. Los clientes activan los bloqueos de retención en función de un MTree. Esto significa que todos los archivos incluidos en un MTree determinado cumplen la definición de bloqueo de retención para ese MTree y establecen la duración de la retención en un nivel por archivo. Una vez que los clientes definen un bloqueo de retención de cumplimiento normativo, ningún usuario ni sistema puede eliminarlo. Un administrador puede revertir un bloqueo de retención de gobernanza, que es la opción menos estricta.[14]

La inmutabilidad de la solución de Rubrik también se basa en los bloqueos de retención para evitar la eliminación o el vencimiento prematuro forzado de las copias de seguridad. Al igual que PowerProtect Cyber Recovery, la solución de Rubrik añade nuevos datos al sistema de archivos en lugar de sobrescribir los datos existentes. La solución almacena los datos entrantes junto con sus huellas digitales. **La solución de Rubrik no habilita los bloqueos de retención de forma predeterminada** y los clientes deben abrir un ticket para solicitar asistencia de Rubrik o habilitar una regla de doble autorización para permitir los bloqueos de retención. (Antes de la versión 7.0 de Rubrik Cloud Data Management, los clientes debían ponerse en contacto con el servicio de asistencia de Rubrik para habilitar los bloqueos de retención; la documentación de Rubrik no deja claro si los clientes pueden ponerse en contacto con el servicio de asistencia para que esto funcione o no). Una vez que los clientes los han habilitado, los bloqueos de retención impiden que los usuarios o los sistemas eliminen datos fuera de los parámetros definidos. Los bloqueos de retención de Rubrik requieren un servidor externo de protocolo de hora de red (NTP) para la sincronización de tiempo, lo que puede dar la oportunidad a los atacantes de manipular la fuente NTP de referencia y, por lo tanto, de que los bloqueos de retención caduquen prematuramente.[15]

> *"La solución de Rubrik no habilita los bloqueos de retención de forma predeterminada y los clientes deben abrir un ticket para solicitar asistencia de Rubrik o habilitar una regla de doble autorización para permitir los bloqueos de retención."*

Licencias y subscripciones

Dell PowerProtect Cyber Recovery es una solución con licencia. Durante la instalación, Dell instala una licencia de evaluación de 90 días de forma predeterminada. Después de 90 días, los clientes deben adquirir una nueva licencia para seguir utilizando el producto. Dell ofrece licencias estándar (permanentes) y licencias basadas en subscripciones.

Rubrik integra Rubrik Cyber Recovery en Rubrik Security Cloud (RSC). Los clientes deben tener una subscripción a Rubrik Enterprise Edition para utilizar Rubrik Cyber Recovery. Los plazos de subscripción son de tres años.[16, 17] En caso de fallo de RSC, las cargas de trabajo de SAP HANA y Db2 requieren herramientas de terceros para recuperar los datos, lo que podría implicar costes de subscripción adicionales.[18]

Acceso de administración

La gestión del sistema Dell PowerProtect Cyber Recovery es local para la topología que elijan los clientes para la implementación. Dado que la solución inicia la recuperación desde el vault, los administradores inician sesión en la interfaz de usuario de gestión desde donde resida su vault. Los vaults en las instalaciones ofrecen a los administradores acceso local sin necesidad de acceso a Internet, que los ciberataques pueden alterar gravemente, ya sea mediante ataques de denegación de servicio o la anulación de la protección de los datos interrumpiendo la conexión a Internet, como recomienda el Instituto Nacional de Normas y Tecnología (NIST). Los vaults ubicados conjuntamente permiten el acceso físico al dispositivo desde un sitio remoto y el uso de conexiones fuera de la red pública de Internet. Los vaults basados en la cloud requerirían acceso a Internet para la recuperación, lo que podría retrasar la recuperación in situ hasta que el ciberataque terminara y se reanudara la conectividad de red normal.

Gestionar Rubrik Cyber Recovery requiere acceso a Rubrik Security Cloud, que requiere acceso a Internet. Como hemos señalado, este tipo de conectividad podría retrasar la recuperación in situ hasta que la funcionalidad de red vuelva a la normalidad tras un ciberataque.

Dado que los clientes deben tener acceso a RSC para utilizar las funciones de Rubrik Cyber Recovery, RSC se convierte en un único punto de fallo. Si ese servicio se volviera inaccesible, dificultaría la recuperación del archivo para el cliente afectado. Rubrik puede recuperar 10 cargas de trabajo durante una interrupción del servicio de RSC, pero dos cargas de trabajo de bases de datos requieren herramientas de terceros y ayuda del servicio de asistencia de Rubrik para su recuperación.[19, 20] Además, las cuentas de administrador comprometidas o los atacantes con acceso a la plataforma RSC obtendrían acceso a todo el entorno y no a un solo vault.

Obtenga ayuda adicional con Managed Detection and Response de Dell

Es posible que algunas organizaciones no se sientan cómodas con un enfoque de ciberseguridad de "hacerlo por su cuenta". Dell ofrece a estos clientes Managed Detection and Response (MDR), un servicio totalmente gestionado que supervisa y detecta amenazas y riesgos y trabaja con los clientes para mitigar dichos riesgos. Según Dell, el servicio ofrece lo siguiente:[21]

- Asistencia de confianza, que incluye asesoramiento de expertos para implementar y configurar las plataformas de análisis de seguridad de detección y respuesta ampliadas (XDR) compatibles con Dell
- Respuesta ante amenazas y configuración de seguridad, incluidas hasta 40 horas de configuración de seguridad relacionada con el servicio incluidas por trimestre.
- Detección e investigación ininterrumpidas, incluida la búsqueda proactiva de amenazas específica para el entorno de cada cliente, a fin de identificar amenazas nuevas o variaciones de las ya conocidas que sorteen los sistemas de seguridad
- Inicio de la respuesta ante incidentes cibernéticos, incluidas 40 horas anuales de asistencia remota para responder ante incidentes, que permite que las actividades de investigación comiencen rápidamente

Cuando se combina con Dell APEX Cyber Recovery Services, MDR permite a los clientes elegir entre muchas opciones para supervisar, detectar y mitigar amenazas y riesgos. La disponibilidad de opciones podría significar una cobertura ampliada o un enfoque híbrido que se adapte a las necesidades de su organización.

Para obtener más información sobre MDR, visite **https://www.dell.com/es-es/lp/dt/managed-detection-response**.

Sin complicaciones

Configuración

La configuración de Dell PowerProtect Cyber Recovery consiste en la instalación de software en un sistema Linux o la creación de un dispositivo VMware® vSphere® a partir de una plantilla de Open Virtualization Format (OVF). La instalación del software requiere 14 pasos,[22] mientras que la implementación alternativa de vSphere Appliance requiere 8 pasos y dura 5 minutos.[23] Después de la instalación, los administradores pueden acceder a la solución a través de navegadores web desde el entorno aislado.

Los clientes deben implementar CyberSense por separado, un motor de análisis de seguridad inteligente totalmente automatizado e integrado.[24] Las instrucciones para instalar CyberSense en Dell PowerProtect Cyber Recovery no están disponibles públicamente.[25]

Dell tiene varias métricas que los usuarios pueden ajustar, como el objetivo de detección de destrucción (DDO), el objetivo de evaluación de destrucción (DAO), el punto de ciberrecuperación (CRP), el tiempo de ciberrecuperación (CRT), el intervalo de sincronización de ciberrecuperación y el recuento de copias de datos de ciberrecuperación. Dell también recomienda caracterizar los datos que necesitan protección. Estos datos pueden ser esenciales, críticos para la empresa, dependientes de los servicios de infraestructura principales u otras aplicaciones, o generales, como binarios de aplicaciones, imágenes de arranque y catálogos de copia de seguridad. La gama de opciones ofrece a los clientes un control total sobre su entorno de copia de seguridad y la capacidad de personalizar la clasificación de sus datos. Dell Consulting Services también puede proporcionar asistencia y sugerencias adicionales.[26]

La configuración de Rubrik también consta de varios pasos. Antes de crear un clúster, los servicios de asistencia de Rubrik deben instalar y configurar Rubrik CDM. A continuación, un administrador descarga e instala la versión más reciente o deseada de CDM (15 pasos).[27] A continuación, el administrador puede configurar un clúster de Rubrik mediante la interfaz de usuario o la CLI. Puede configurar el clúster con la interfaz de usuario o la CLI, y ambos enfoques siguen 24 pasos.[28, 29] A continuación, el administrador puede registrar los clústeres de Rubrik utilizando un método en línea (12 pasos)[30] o un método sin conexión (18 pasos).[31] A continuación, el administrador habilita la autenticación multifactor (MFA), que requiere 13 pasos.[32] Por último, el administrador añade la cuenta inicial (6 pasos) y cualquier otra cuenta.[33] En la Figura 3 se muestra el número máximo de pasos posibles para configurar cada solución de ciberrecuperación.

Los clientes de Rubrik no pueden ajustar otras métricas, lo que podría reducir la flexibilidad para satisfacer sus necesidades. Según un evaluador: "La mayor parte de la interfaz de usuario es bastante sencilla e intuitiva, pero en algunas áreas se echa de menos una descripción más detallada de la función de la opción o la opción no está presente. Si bien facilita la experiencia del usuario, se echan en falta muchos ajustes y se requiere abrir un túnel al servicio de asistencia para que un especialista realice un cambio en el entorno del cliente".[34]

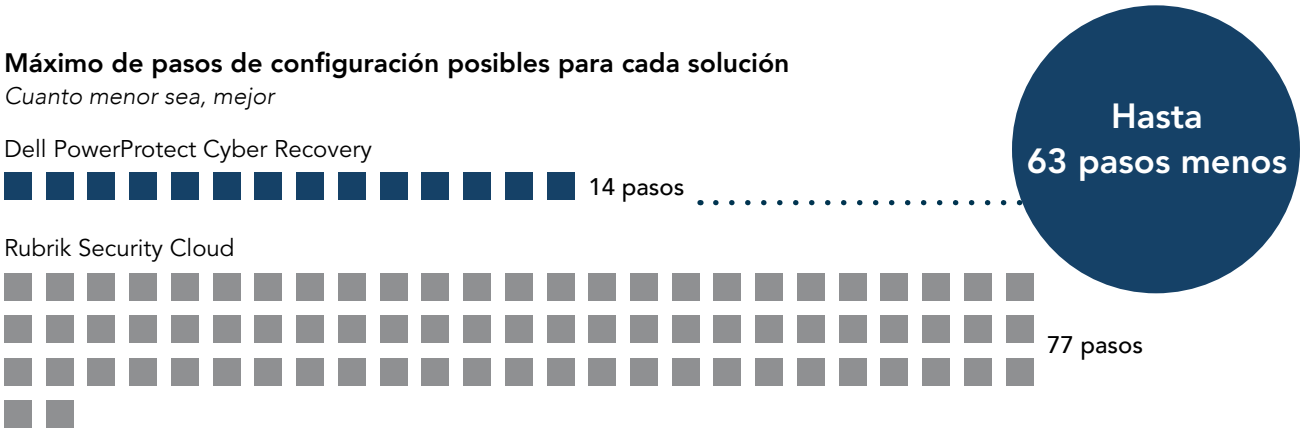

Figura 3: El número máximo de pasos posibles para configurar Dell PowerProtect Cyber Recovery y Rubrik Security Cloud. Cuanto más bajo es mejor. Fuente: Principled Technologies.

Mantenimiento

Hemos observado que después de la configuración, las IU de Dell y Rubrik para realizar operaciones de mantenimiento diarias son similares. Después de la configuración, los clientes pueden configurar Dell PowerProtect Cyber Recovery para hacer lo siguiente:[35] [36]

- Generar automáticamente informes de trabajos de Cyber Recovery de acuerdo con un programa y en respuesta a una solicitud manual del usuario
    - Un usuario o programa crea trabajos cuando inicia una política, una operación de recuperación, una copia de seguridad del sistema o una operación de limpieza.
- Supervisar automáticamente el estado del vault, la capacidad de almacenamiento, las operaciones de Cyber Recovery, las alertas cuando falla la copia/sincronización o si el vault de Cyber Recovery está inactivo y los trabajos de Cyber Recovery
- Buscar ataques de forma automática y continua y mostrar alertas de CyberSense tras ellos, por orden de gravedad e indicando el número de archivos, hosts, políticas afectadas, amenazas específicas detectadas, el punto en el tiempo del ataque para que pueda encontrar una copia de seguridad limpia y una lista de archivos dañados para utilizar en el análisis de ataques

Del mismo modo, los clientes pueden configurar Rubrik para que realice lo siguiente:[37]

- Utilizar Rubrik Security Cloud automáticamente para rastrear, supervisar y mostrar todos los eventos de todos los clústeres de Rubrik conectados. Proporciona tres tipos de eventos:[38]
    - Críticos: eventos que requieren atención, como una copia de seguridad fallida, una operación de archivo o una replicación
    - Advertencia: se ha finalizado una copia de seguridad, una operación de archivo o una recuperación
    - Informativo: solo información
- Analizar instantáneas de forma automática y continua en busca de indicadores de riesgo nuevos y existentes mediante Threat Monitor, que indica el momento en que la solución tomó por última vez una instantánea, la línea de tiempo del evento, el tiempo de detección, el número de archivos modificados, el número de archivos sospechosos, el nombre del clúster y el tipo y el nombre de objeto

Admisión de cargas de trabajo de anomalías

Tanto el análisis de amenazas de datos en la cloud de seguridad de Rubrik como CyberSense analizan varios tipos de cargas de trabajo, pero según las fuentes que encontramos, CyberSense admite dos veces más cargas de trabajo de detección de anomalías. Esto incluye analizar los siguientes tipos de cargas de trabajo:

- Máquinas virtuales
- Infraestructura básica
- Archivos de usuario que pueden contener documentos, contratos y propiedad intelectual
- Bases de datos
- Copias de seguridad realizadas por otros clientes

"Si contamos el número de cargas de trabajo admitidas que encontramos en los datos disponibles públicamente, encontramos que CyberSense admite 21 cargas de trabajo de detección de anomalías, mientras que Rubrik admite 7."

Si contamos el número de cargas de trabajo admitidas que encontramos en los datos disponibles públicamente, encontramos que CyberSense admite 21 cargas de trabajo de detección de anomalías, mientras que Rubrik admite 7. Por lo tanto, según los datos disponibles públicamente compartidos por cada uno, CyberSense admite dos veces más cargas de trabajo que Rubrik Security Cloud Data Threat Analytics. Cuantos más datos pueda analizar una solución de ciberrecuperación, mejor será la probabilidad de encontrar malware sigiloso u otros daños.

Admisión de cargas de trabajo de máquinas virtuales

Las cargas de trabajo de máquinas virtuales se refieren a las aplicaciones, los servicios o las tareas que ejecutan las máquinas virtuales en un servidor host físico o un entorno de cloud. Debido a que estas cargas de trabajo pueden variar en su función y de muchas otras formas que podrían dar lugar a una mayor exposición al malware, es esencial analizar las máquinas virtuales. Rubrik Security Cloud Data Threat Analytics, que "comprende la detección de anomalías, la supervisión de amenazas, la búsqueda de amenazas y los servicios de recuperación de datos en recursos protegidos",[39] admite el análisis de las siguientes cargas de trabajo de máquinas virtuales:[40]

- VMware
- Nutanix® AHV
- Microsoft Hyper-V
- Microsoft Azure

CyberSense admite el análisis de las siguientes cargas de trabajo de máquinas virtuales:[41, 42, 43]

- VMware
- Amazon Web Services (AWS)
- Hyper-V, con copias de seguridad de Dell Avamar o Dell NetWorker

VMware afirma que "hasta el 80 % de las cargas de trabajo virtualizadas se ejecutan en tecnología de VMware".[44] En el primer trimestre de 2024, Amazon Web Services (AWS), el proveedor más popular en el mercado de servicios de infraestructura de cloud, controló el 31 % de todo el mercado. Microsoft Azure ocupa el segundo lugar con una cuota de mercado del 25 %.[45]

Infraestructura básica

La infraestructura básica son los componentes y servicios fundamentales que permiten el funcionamiento de un entorno tecnológico. La detección de malware a este nivel puede ayudar a reducir la gravedad de un ataque, ya que la funcionalidad principal de la infraestructura puede afectar a muchos sistemas y usuarios. La documentación de Rubrik Security Cloud no menciona la admisión del análisis de cualquier infraestructura principal.[46]

Por el contrario, CyberSense admite el análisis de la siguiente infraestructura básica:[47]

- Active Directory
- DNS
- LDAP

Archivos de usuario que pueden contener documentos, contratos y propiedad intelectual

Rubrik Security Cloud Data Threat Analytics admite el análisis de los siguientes archivos de usuario:[48]

- Conjuntos de archivos y conjuntos de datos NAS
- Grupos de volúmenes de Windows
- Linux y Windows

CyberSense puede analizar archivos de usuario de Linux y Windows.[49]

Análisis de bases de datos

CyberSense 7 frente a RSC Data Threat Analytics 0

Bases de datos

Las aplicaciones pueden utilizar diferentes tipos de bases de datos por muchas razones, por lo que ser capaz de detectar la presencia de malware en varias bases de datos podría ser fundamental para una respuesta rápida. Rubrik Security Cloud Data Threat Analytics puede realizar copias de seguridad de bases de datos, pero no encontramos documentación pública en la que puedan analizar esas copias de seguridad de bases de datos.

CyberSense admite el análisis de las siguientes bases de datos con análisis a nivel de página:[50]

- SQL
- Oracle®
- SAP HANA
- Db2
- PostgreSQL
- Epic® Caché
- MariaDB/MySQL

Copias de seguridad realizadas por otros clientes

Algunas organizaciones pueden tener copias de seguridad de datos de varios proveedores para proporcionar redundancia, cumplir normativas o por alguna otra razón significativa. La documentación de Rubrik Security Cloud no menciona la admisión del análisis de copias de seguridad realizadas por otros clientes de copia de seguridad.[51]

Con una clara ventaja en esta categoría, CyberSense admite el análisis de copias de seguridad realizadas por los siguientes clientes de copia de seguridad:[52, 53, , 54]

- DNAS
- SQL
- NetWorker
- Veritas NetBackup
- Exchange
- Avamar
- Commvault

Tecnología de análisis

Rubrik Security Cloud incluye muchas herramientas para analizar y ayudar con el análisis en Data Threat Analytics:

- Rubrik Anomaly Detection muestra archivos sospechosos, cambios en las instantáneas y[55] detalles de anomalías como incidentes de anomalías para que los clientes los estudien y utilicen en la investigación de instantáneas.[56] El software también proporciona opciones de recuperación.[57]
- Rubrik VM Encryption Detection detecta ataques en los archivos de disco virtual de VMware vSphere.[58]
- Rubrik Threat Monitoring muestra información sobre las amenazas y coincidencias detectadas.[59]
- Rubrik Threat Hunt es un análisis iniciado por el usuario en busca de indicadores de riesgo.[60]
- Rubrik Quarantine aísla los objetos que aparecen en una búsqueda de amenazas.[61]

Rubrik RSC también cuenta con conectores de servicio de copia de seguridad de Rubrik para cada clúster de Rubrik.

Los clientes de Rubrik deben seleccionar la herramienta correcta para su tarea. Es posible que tengan que iniciar los análisis manualmente o utilizar varias herramientas para llevar a cabo dicha tarea. Por el contrario, Dell tiene una única opción de análisis con CyberSense, que los clientes pueden encontrar más fácil de gestionar y administrar.

El análisis de CyberSense es más profundo que el análisis "solo superficial" de Rubrik RSC Data Threat Analytics. CyberSense realiza análisis de contenido completo de los archivos y análisis a nivel de página de las bases de datos, y puede detectar el cifrado parcial de los archivos.[62] La herramienta utiliza una base de datos de aprendizaje automático (ML) entrenada por Index Engines sobre miles de amenazas de datos y contiene más de 200 puntos de análisis para detectar la corrupción de datos.[63] A diferencia de Rubrik Threat Monitoring y Threat Hunt, CyberSense no depende de agencias externas de inteligencia de amenazas para obtener firmas de malware. En su lugar, detecta nuevas amenazas.[64] **CyberSense tampoco se basa en umbrales arbitrarios de cambios aceptables en los archivos o niveles de entropía entre instantáneas que puedan dar lugar a falsos negativos**, ni entrena su aprendizaje automático con respecto a una referencia del comportamiento previo del cliente.[65, 66, 67]

El software de detección de anomalías de Rubrik se basa únicamente en metadatos para determinar si una instantánea está dañada antes de realizar cualquier análisis de contenido. En comparación con el ML continuo de CyberSense, el software de Rubrik detecta daños después de obtener firmas. La detección de anomalías de Rubrik precisa crear un modelo de comportamiento para definir la referencia normal de un cliente. Esto puede tardar varias copias de seguridad en establecerse. El modelo de comportamiento de Rubrik requiere al menos dos copias de seguridad para crear una referencia de cambios típicos en un sistema de archivos cuando no hay ataques. Sin embargo, un conjunto único de estadísticas de cambio podría no ser suficiente para establecer lo que es típico. Los eventos empresariales podrían desencadenar más o menos actividad o tipos de actividad más sospechosos que no ocurrieron entre la primera y la segunda instantánea

> *"CyberSense tampoco se basa en umbrales arbitrarios de cambios aceptables en los archivos o niveles de entropía entre instantáneas que puedan dar lugar a falsos negativos...."*

de Rubrik. Cuantas más copias de seguridad analice la solución de Rubrik, con mayor precisión podrá entrenar su modelo de comportamiento conforme a una referencia.[68, 69]

CyberSense contiene todos sus análisis en el vault. En el pipeline de análisis del comportamiento del sistema de archivos, Rubrik envía metadatos sobre los cambios en el sistema de archivos del cliente a la plataforma Polaris basada en la cloud para realizar el análisis del comportamiento, lo que abre una superficie de ataque.[70]

Los clientes pueden utilizar Rubrik Threat Monitoring y Threat Hunt solo como parte de la edición Rubrik Enterprise.[71] Los clientes deben realizar análisis de Threat Hunt con privilegios de control de acceso basado en funciones (RBAC) y los usuarios deben indicar qué indicadores de riesgo (IOC) específicos desean buscar.[72] Esta no es una práctica recomendada en el sector.[73] Al igual que CyberSense, Threat Hunt es compatible con VMware, AHV, Hyper-V, conjuntos de archivos NAS y servidores Linux y Windows.[74]

En las siguientes secciones se ofrecen más detalles sobre cómo la solución de Rubrik ofrece la detección de amenazas.

Metadatos y estadísticas del sistema de archivos

El modelo de comportamiento de aprendizaje automático de Rubrik Anomaly Detection registra los cambios en el sistema de archivos desde la última instantánea (como el número de archivos añadidos, eliminados o movidos) como metadatos.[75] Entonces, un modelo de aprendizaje automático se entrena conforme a estos cambios para crear un modelo de comportamiento "de referencia" para el sistema de archivos. Rubrik marca una instantánea como anómala si detecta demasiados cambios. Una vez que el análisis de comportamiento ha marcado una instantánea, la solución inicia un análisis de contenido de archivos.[76] La supervisión de los metadatos puede añadir una capa de seguridad, pero es posible que no ofrezca la protección necesaria que ayude a prevenir o reducir el tiempo de inactividad de un evento.

Por el contrario, **CyberSense no necesita una referencia; supervisa y analiza los cambios en el contenido de archivos y bases de datos desde las primeras copias de seguridad.** El enfoque de CyberSense ofrece más granularidad, ya que el software analiza incluso fragmentos de un archivo o páginas individuales de una base de datos. Al igual que con la solución de Rubrik, los análisis de CyberSense incluyen propiedades de metadatos y alimentan el motor de ML con los resultados. A diferencia de la solución de Rubrik, CyberSense no se limita al análisis de metadatos, e Index Engines entrenó su motor de ML con ataques documentados por Index Engines, no con firmas ni con un comportamiento previo del cliente.[77, 78]

> *"CyberSense no necesita una referencia; supervisa y analiza los cambios en el contenido de archivos y bases de datos desde las primeras copias de seguridad."*

Umbrales

Durante el análisis del comportamiento, el aprendizaje automático de Rubrik determina la probabilidad de que se produzca una anomalía en un sistema de archivos. Si la solución de Rubrik lo considera probable, realiza análisis de contenido. Esto podría ser un umbral determinado por el modelo de comportamiento para el "comportamiento anómalo". Por ejemplo, la solución de Rubrik podría marcar un comportamiento anómalo cuando observa muchos archivos nuevos o modificados, o un aumento de aleatoriedad o indicadores de cifrado.[79] Durante el análisis de contenido, Rubrik Anomaly Detection muestra los cambios en el contenido de los archivos y calcula la probabilidad de cifrado mediante el cálculo de la entropía del sistema de archivos. La entropía de un sistema de archivos ayuda a mostrar la probabilidad de que un ataque de ransomware tenga archivos cifrados. Si la entropía supera un umbral de anomalías, la solución alerta al usuario.[80, 81] La eficacia en la detección de daños en los datos depende de la rigidez del umbral. Demasiado margen podría dar lugar a falsos negativos y, por lo tanto, a una falsa sensación de seguridad.[82] Los clientes deben establecer los umbrales de forma adecuada.

Por el contrario, CyberSense comprueba el cifrado parcial de un archivo mediante el análisis del contenido del archivo para proporcionar una confianza del 99,99 % (según Dell e Index Engines) en la detección de daños en los datos.[83]

Firmas y extensiones de archivos

Rubrik Threat Monitoring y Threat Hunts analizan instantáneas de IOC. Cuando una de las diversas fuentes de inteligencia contra amenazas que Rubrik supervisa descubre un nuevo IDC, Threat Monitoring envía la fuente de amenazas que contiene otras reglas Yet Another Ridiculous Acronym (YARA u "Otro Acrónimo Ridículo" en español) para identificar el nuevo malware, también conocido como la firma de malware, a todos los clústeres de Rubrik. A continuación, los clústeres comienzan a analizar.[84] Un informe reciente de WatchGuard sugiere que el 57,8 % del malware evita la detección de firmas. El malware avanzado, como BianLian, puede emplear métodos para evadir el reconocimiento de firmas y las nuevas variantes de malware pueden tener firmas ligeramente diferentes de las originales. Por lo tanto, podría ser más difícil para la inteligencia contra amenazas mantenerse actualizada.[85]

En comparación, CyberSense utiliza más de 200 análisis y proporciona un modelo de aprendizaje automático entrenado en miles de variantes de ransomware. Index Engines ha demostrado que el método de CyberSense puede detectar variantes previamente desconocidas y sofisticadas sin descargar firmas,[86] lo que es otra ventaja de no depender de Internet durante un evento.

Eventos de cifrado masivo

La solución de Rubrik supervisa los eventos de cifrado masivo mediante el cálculo de la entropía de todo el sistema de archivos.[87] CyberSense es mucho más granular. No solo analiza el sistema de archivos en general, o incluso cada archivo individual, sino que analiza partes del contenido interno de los archivos. Según Index Engines, el cálculo de la entropía en solo un archivo completo en lugar de fragmentos de él "solo detectará el cifrado extremo de todo el archivo", o eventos de cifrado masivo.[88]

Capacidad de recuperación

Según la documentación, consideramos que la recuperación con Dell PowerProtect Cyber Recovery es un proceso más sencillo y optimizado que la recuperación con Rubrik. En esta sección del informe, incluidas sus subsecciones, se comparan las funciones de recuperación de las dos soluciones y cómo las soluciones implementan dichas funciones.

La documentación de Rubrik indica cuáles de sus funciones de recuperación funcionan para qué tipos de máquinas virtuales. Puede parecer que ofrece un nivel útil de granularidad, pero las numerosas estipulaciones y variaciones hacen que la recuperación sea compleja. Por ejemplo, cuando los clientes de Rubrik necesitan recuperar datos, archivos y sistemas, deben seleccionar los objetos de instantánea que desean incluir en su plan de recuperación. Después de crear uno o más planes de recuperación, Rubrik ofrece muchas opciones de recuperación, entre las que se incluyen las siguientes:[89, 90, 91, 92, 93]

- Recuperación de archivos a través de la descarga o sobreescritura y recuperación en una carpeta independiente, exportación a un host diferente o exportación a un servicio de clúster
- Recuperación de archivos para máquinas virtuales a través de la descarga o sobreescritura y recuperación en una carpeta independiente o exportación a otra máquina virtual
- Recuperación completa de la instantánea de una máquina virtual o instantánea de disco a través de lo siguiente:
  - Montaje en directo, que crea una nueva máquina virtual a partir de la instantánea
  - Montaje de discos virtuales, que crea discos virtuales nuevos a partir de la instantánea
  - Recuperación instantánea, que reemplaza la máquina virtual actual por una nueva máquina virtual creada a partir de la instantánea
  - Exportación, que crea una nueva máquina virtual a partir de la instantánea en un almacén de datos seleccionado
  - Recuperación por lotes de máquinas virtuales
- Ciberrecuperación masiva para planes de recuperación a través del montaje en directo y la exportación
- Recuperación coordinada de aplicaciones de Rubrik Security Cloud para la recuperación ante desastres de máquinas virtuales en un entorno aislado, un sitio remoto o en las instalaciones

La recuperación por lotes de Rubrik demuestra ser aún más compleja. En la Tabla 1 se muestran las funciones de recuperación por lotes que Rubrik proporciona en función del hipervisor.[94]

Tabla 1: Características de recuperación por lotes que Rubrik proporciona para diferentes hipervisores. Fuente: Rubrik.

Opciones de creación de máquinas virtuales				
	Montaje en directo	**Montaje en directo con migración opcional**	**Exportar**	**Recuperación instantánea**
Máquinas virtuales vSphere	Disponible, utiliza el clúster de Rubrik como almacén de datos.	No disponible	Disponible, utiliza el almacén de datos del hipervisor recuperado.	Disponible, utiliza el clúster de Rubrik como almacén de datos.
Máquinas virtuales AHV	Disponible, utiliza el clúster de Rubrik como almacén de datos.	Disponible, utiliza el clúster de Rubrik como almacén de datos y utiliza el contenedor de Nutanix para todas las escrituras posteriores.	Disponible, utiliza el contenedor de Nutanix como almacén de datos.	No disponible
Máquinas virtuales Hyper-V	Disponible, utiliza el clúster de Rubrik como almacén de datos.	No disponible	Disponible, utiliza el almacén de datos del hipervisor recuperado.	Disponible, reemplaza la máquina virtual actual por una nueva a partir de la instantánea. Utiliza el clúster de Rubrik como almacén de datos.

En el caso de la solución de Rubrik, el almacén de datos recuperado suele estar en el clúster de Rubrik y no en el entorno de producción, lo que puede crear problemas. Presentamos estos problemas en la siguiente sección, "Limitaciones de Rubrik". Por el contrario, PowerProtect puede colocar los datos recuperados en entornos de recuperación o producción para ayudar a proporcionar una recuperación más rápida y fluida que podría minimizar el tiempo de inactividad.

En la Tabla 2 se muestra información adicional de Rubrik sobre la recuperación de máquinas virtuales de vSphere.[95] Como se muestra en la tabla, la mayoría de los almacenes de datos de recuperación de vSphere se encuentran en el clúster de Rubrik.

Tabla 2: Funciones de recuperación que Rubrik proporciona para las máquinas virtuales vSphere. Fuente: Rubrik.

Funciones de recuperación que Rubrik proporciona para vSphere				
Acción	**Almacén de datos**	**Estado de alimentación**	**Red**	**Máquina virtual de origen**
Recuperación de archivos	No aplicable	No aplicable	No aplicable	Ningún impacto
Montaje en directo	Clúster local de Rubrik	Activado o desactivado	Desconectado	Ningún impacto
Montaje de discos virtuales	Clúster local de Rubrik	Activado	Desconectado	Ningún impacto
Recuperación instantánea	Clúster local de Rubrik	Activado	Conectado (opcional)	Apagada y con cambio de nombre
Exportar	Almacén de datos del hipervisor	Desactivado	Desconectado	Ningún impacto
Recuperación in situ	Almacén de datos del hipervisor	Activado	Igual que la máquina virtual de origen	La recuperación in situ sobrescribe los archivos de disco virtual de la máquina virtual de origen con los datos de disco virtual de la instantánea, sin cambiar las propiedades de la máquina virtual.

La solución de Rubrik no implementa en general la recuperación masiva y las opciones de recuperación masiva son limitadas y complejas. Como se explica en la sección "Dell PowerProtect Data Manager ofrece la función equivalente a la "restauración masiva" de Rubrik." de este informe, Dell PowerProtect es más optimizado y sencillo.

Desmitificación de la restauración masiva

Rubrik anuncia la recuperación masiva, que define como la restauración rápida de las operaciones empresariales mediante la recuperación de aplicaciones, archivos o usuarios a escala.[96] Ofrece muchas opciones de recuperación masiva. Sin embargo, la solución de Rubrik generalmente almacena los datos recuperados en el clúster de Rubrik y no en el entorno de producción.[97] Las cargas de trabajo dependen de la disponibilidad del sistema de Rubrik hasta que la solución complete su migración. El clúster local de Rubrik es de almacenamiento de nivel 3, por lo que los clientes tendrían que realizar una migración adicional a su entorno de producción para volver a los niveles de rendimiento planificados. Con este único punto de fallo y un rendimiento reducido mientras el sistema completa la migración, no podemos considerar la recuperación completa hasta que la solución de Rubrik restaure las cargas de trabajo en el entorno de producción.

Dell PowerProtect también ofrece la recuperación masiva al permitir a los usuarios seleccionar varias máquinas virtuales para la recuperación en su interfaz de usuario de recuperación.

Dell PowerProtect Data Manager ofrece la función equivalente a la "restauración masiva" de Rubrik.

En comparación con la solución de Rubrik, la solución de Dell también ofrece varias opciones de recuperación equivalentes para máquinas virtuales de vSphere. Dell PowerProtect puede colocar datos de máquinas virtuales en entornos de recuperación o producción. La mayoría de las opciones de Rubrik colocan los datos solo en el clúster de Rubrik. En la Tabla 3 se muestran las opciones de recuperación de Dell.[98, 99, 100, 101]

Tabla 3: Opciones de recuperación de Dell. Fuente: Principled Technologies.

Opciones de recuperación de Dell	
Tipo	**Acerca de la función**
Restauración a nivel de archivo	Restaura solo los archivos infectados en su lugar o mediante reversión.
VM en directo	Restaura una máquina virtual en el clúster con una migración posterior a la producción.
Restauración a nuevo	Restablece al entorno original o a un nuevo entorno (por ejemplo, un cuarto limpio o una infraestructura de recuperación). Durante la restauración, los usuarios pueden seleccionar varias máquinas virtuales al mismo tiempo para que la restauración sea masiva o a gran escala.
Acceso/VM en directo	Crea una copia aislada de los datos de producción.
Coordinación de recuperación	Permite a los administradores programar la recuperación u ofrecerla bajo demanda; prioriza la recuperación automática de las máquinas virtuales en el entorno de producción o recuperación.

Limitaciones de Rubrik

La solución de Rubrik pone en cuarentena las instantáneas infectadas con malware para análisis futuros. Sin embargo, la solución de Rubrik no pone en cuarentena las instantáneas de forma predeterminada. A continuación, los clientes pueden descargar y realizar análisis forenses de los archivos en cuarentena ellos mismos manualmente o con herramientas de terceros, lo que podría exponerles a malware.[102, 103]

> *CyberSense realiza su análisis sin necesidad de que el usuario realice su propio análisis forense y el software automatiza la creación de puntos de restauración.*

CyberSense analiza archivos y bases de datos de forma predeterminada. Los usuarios no necesitan poner en cuarentena las instantáneas manualmente. **CyberSense realiza su análisis sin necesidad de que el usuario realice su propio análisis forense y el software automatiza la creación de puntos de restauración.**[104]

Rubrik RSC en modo de gestión solo de RSC es un punto de fallo único de muchas características. Lo más preocupante es que un ataque podría provocar una interrupción del servicio de RSC que afecte a la conectividad a Internet del usuario o a la conectividad entre el sitio del usuario y el RSC. Después de estos ataques, la solución proporciona un conjunto limitado de funciones a los usuarios, disponibles a través de la automatización basada en API o la interfaz de usuario de Rubrik CDM, pero solo si los usuarios crearon una cuenta de servicio de RSC antes del ataque.[105] [106] Una organización puede recuperar las siguientes cargas de trabajo y datos sin el servicio de RSC: MongoDB, Microsoft Exchange, archivos, instantáneas de Hyper-V, montaje en directo de volúmenes gestionados, archivos del host NAS, Oracle, SQL Server, VCD y VMware.[107] La recuperación de SAP HANA sin el servicio de RSC requiere herramientas de terceros, como Studio y Cockpit Cross, y el servicio de asistencia de Rubrik a través del túnel al servicio de asistencia. La recuperación de IBM Db2 sin el servicio de RSC requiere herramientas de terceros de IBM y el servicio de asistencia de Rubrik a través del túnel al servicio de asistencia.[108]

Cámara de aire/aislamiento

El NIST define la cámara de aire como "una interfaz entre dos sistemas en la que (a) no están conectados físicamente y (b) ninguna conexión lógica no está automatizada (es decir, los datos se transfieren a través de la interfaz solo manualmente, bajo control humano)".[109]

Las cámaras de aire pueden ayudar a controlar el flujo de datos de un origen a un destino y pueden ser un componente importante de cualquier estrategia de protección contra ransomware y de ciberrecuperación. Si un ataque o evento pone en peligro los sistemas de copia de seguridad de producción, la capacidad de evitar el tráfico desde los sistemas de producción a copias de seguridad protegidas en los vaults de ciberrecuperación podría ofrecer una seguridad a prueba de fallos.

Aislamiento físico

Puede que haya visto un ejemplo de una solución físicamente aislada en la película Misión imposible, donde el protagonista tuvo que eludir todas las demás funciones de seguridad de las instalaciones para acceder a datos confidenciales en un sistema informático que no estaba conectado a ninguna red externa. El aislamiento físico también puede utilizar segmentos normalmente desconectados de una red física específica para transportar copias de seguridad desde los sistemas de producción hasta el vault. Cuando están desconectados, estas cámaras de aire operativas crean una barrera física que los datos no pueden cruzar automáticamente, lo que dificulta el acceso de los atacantes.

Las organizaciones pueden aislar físicamente Dell PowerProtect Cyber Recovery para ayudar a aplicar una estrategia de cámara de aire operativa. La solución utiliza una conexión física específica y realiza la replicación de datos como una operación de extracción desde el vault en lugar de una operación de inserción desde la solución de copia de seguridad. Durante la copia o replicación, la solución activa la conexión, cifra los datos y los migra a través de la línea específica.[110] Después de completar la replicación, la solución vuelve a desactivar la conexión desde el lado del vault. La solución hace que las copias del vault sean inmutables con políticas de retención bloqueadas, de modo que, incluso si un usuario o sistema obtiene acceso, no pueda modificar ni eliminar las copias del vault. Ningún tráfico de gestión atraviesa la ruta de replicación,

por lo que **incluso si los atacantes obtienen el control de la solución de copia de seguridad en las instalaciones, el vault inicia y desconecta la ruta de replicación y utiliza extracciones unidireccionales de solo datos del origen de datos, lo que limita el acceso directo al vault.**[111]

Aislamiento lógico

El aislamiento lógico, por otro lado, utiliza sistemas que pueden residir en la misma red física, pero crea una separación y control lógicos de la red para garantizar que los sistemas no puedan enviar datos entre sí. La solución utiliza implementaciones de seguridad adicionales, como el cifrado y el hashing, junto con el RBAC y la autenticación multifactor, para garantizar que un sistema o usuario no autorizado no pueda leer los datos que residen en otro sistema.

Rubrik describe su función de ciberrecuperación como el aprovechamiento de una estrategia de cámara de aire lógica.[112, 113] Muchas de las declaraciones públicas de Rubrik disponibles ponen en duda la necesidad de las cámaras de aire. Según una presentación de Rubrik titulada "Rubrik Security – Air Gap and Inmutability", su solución nativa está aislada, porque no hay forma de acceder o editar las copias de seguridad una vez que la solución las toma, incluso si el dispositivo Rubrik permanece en la red física.[114] Sin embargo, un atacante autenticado podría obtener acceso a la GUI del dispositivo, lo que podría tener ramificaciones para la recuperación. Para mitigar esto, Rubrik tiene bloqueos de retención que impiden el vencimiento de las copias de seguridad, lo que las hace inmutables. Una vez habilitados, los bloqueos de retención también impiden que un clúster de Rubrik se restablezca de fábrica y se borre. Según la guía de seguridad de Rubrik CDM, la solución deshabilita globalmente los bloqueos de retención en el clúster de forma predeterminada y requiere que los clientes se pongan en contacto con el servicio de asistencia de Rubrik para habilitarlos.[115] Las fuentes disponibles públicamente no aclaran si el servicio de asistencia de Rubrik también puede deshabilitar los bloqueos de retención, lo que plantea la posibilidad de que un atacante autorizado aún pueda eludir las capas de seguridad.

> *"Ningún tráfico de gestión atraviesa la ruta de replicación, por lo que incluso si los atacantes obtienen el control de la solución de copia de seguridad en las instalaciones, el vault inicia y desconecta la ruta de replicación y utiliza extracciones unidireccionales de solo datos del origen de datos, lo que limita el acceso directo al vault."*

Conclusión

Las organizaciones deben considerar activamente numerosos vectores de ataque en sus centros de datos. Un buen plan de protección de datos busca proteger todos los datos, en particular los datos críticos fundamentales para las operaciones. Analizamos la información disponible públicamente sobre Dell PowerProtect Cyber Recovery y Rubrik Secure Cloud para ver cómo ambas soluciones abordan la gestión, la protección y la recuperación de datos.

PowerProtect Cyber Recovery aísla físicamente las copias de seguridad de los datos críticos en un vault y garantiza su capacidad de recuperación en caso de ciberataque. La solución aplica una estrategia de cámara de aire operativa con aislamiento físico, algo que Rubrik Secure Cloud no puede afirmar, ya que la solución se basa en el aislamiento lógico.

Cyber Recovery utiliza análisis basados en ML en CyberSense para evaluar la integridad de los datos en el vault e identificar datos limpios de copia de seguridad para la recuperación. Rubrik Secure Cloud, por el contrario, ofrece una herramienta de análisis entrenada en ML que busca anomalías en lugar de realizar análisis profundos de archivos.

Además, la solución Cyber Recovery ofrece varias opciones de recuperación, que aprovechan los datos no comprometidos del vault para permitir reanudar el funcionamiento de forma eficiente y fluida. En muchos casos, PowerProtect Cyber Recovery podría ofrecer características y ventajas de las que Rubrik Secure Cloud carece, lo que ofrece una solución potencialmente más segura y capaz de analizar más a fondo para minimizar el tiempo de inactividad y acelerar la recuperación.

---

1. Anastasia Dergacheva y Jesse R. Taylor, "Study Finds Average Cost of Data Breaches Continued to Rise in 2023", acceso el 25 de julio de 2024, https://www.morganlewis.com/blogs/sourcingatmorganlewis/2024/03/study-finds-average-cost-of-data-breaches-continued-to-rise-in-2023.
2. Dell, "Dell PowerProtect Cyber Recovery Solution Guide", acceso el 18 de abril de 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
3. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".
4. Rubrik, "Rubrik Security Cloud Architecture and Security Implementation", acceso el 18 de abril de 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf.
5. Rubrik, "Dell PowerProtect Cyber Recovery Solution Guide", acceso el 18 de abril de 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf.
6. Rob Emsley, "Public Cloud Vault to Secure, Isolate and Recover Data", acceso el 20 de marzo de 2024, https://www.dell.com/en-us/blog/public-cloud-vault-to-secure-isolate-and-recover-data/.

7. Brian White, "Dell's PowerProtect Cyber Recovery Expands to Microsoft Azure", acceso el 20 de marzo de 2024, https://www.dell.com/en-us/blog/dells-powerprotect-cyber-recovery-expands-to-microsoft-azure/.
8. Dell, "Cyber Recovery on Google Cloud Platform", acceso el 20 de marzo de 2024, https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-cyber-recovery-reference-architecture/cyber-recovery-on-google-cloud-platform/.
9. Chris Mellor, "Up to $5m compensation if Rubrik Cloud Vault recovery busted", acceso el 20 de marzo de 2024, https://blocksandfiles.com/2022/02/24/up-to-5m-compensation-if-rubrik-cloud-vault-recovery-busted/.
10. Kristina Avrionova, "Frequently Asked Questions about Rubrik Cloud Vault", acceso el 20 de marzo de 2024, https://www.rubrik.com/blog/company/22/3/faq-about-rubrik-cloud-vault.
11. Chris Wahl, "Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture", acceso el 22 de marzo de 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf.
12. Dell, "Data Domain Invulnerability Architecture: Enhancing Data Integrity and Recoverability", acceso el 7 de junio de 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h7219-data-domain-data-invul-arch-wp.pdf.
13. Dell, "Consolidate Governance and Compliance Archive Data", acceso el 4 de abril de 2024, https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-domain-retention-lock/consolidate-governance-and-compliance-archive-data/.
14. Dell, "Dell PowerProtect Cyber Recovery Solution Guide", acceso el 24 de marzo de 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
15. Rubrik, "Retention-locked SLA Domain attributes", acceso el 2 de abril de 2024, https://docs.rubrik.com/es-es/8.0/ug/cdm/atributos_de_dominios_de_sla_con_retencion_bloqueada.html.
16. Rubrik, "Rubrik Cyber Recovery", acceso el 20 de marzo de 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/brf-rubrik-cyber-recovery.pdf.
17. Rubrik, "Rubrik Licensing: Subscribe to Simplicity", acceso el 20 de marzo de 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/data-sheet/rubrik-licensing-data-sheet.pdf.
18. Rubrik, "Workloads require third-party tools for recovery", acceso el 6 de mayo de 2024, https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html .
19. Rubrik, "Recoverable workloads during RSC service disruption", acceso el 6 de mayo de 2024, https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html.
20. Rubrik, "Workloads require third-party tools for recovery".
21. Dell, "Refuerce el estado de seguridad con Managed Detection and Response", acceso el 2 de abril de 2024, https://www.delltechnologies.com/asset/es-es/services/managed-services/technical-support/managed-detection-and-response-datasheet.pdf.
22. Dell, "Dell PowerProtect Cyber Recovery 19.13 Installation Guide", acceso el 20 de marzo de 2024, https://www.dell.com/support/manuals/es-es/cyber-recovery/irs_p_19.13_installation/installing-the-cyber-recovery-software?guid=guid-8718978d-ddd0-4dc0-bca7-fb04a2f3d1fb&lang=en-us.
23. Dell, "Dell PowerProtect Cyber Recovery 19.13 Installation Guide".
24. Dell, "Dell PowerProtect Cyber Recovery 19.13 Installation Guide".
25. Dell, "Installing CyberSense in Dell PowerProtect Cyber Recovery", acceso el 20 de marzo de 2024, https://infohub.delltechnologies.com/en-US/l/ransomware-protection-secure-your-data-on-dell-powerflex-with-powerprotect-cyber-recovery-1/installing-cybersense-in-dell-powerprotect-cyber-recovery-1/.
26. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".
27. Rubrik, "Downloading and installing Rubrik CDM", acceso el 20 de marzo de 2024, https://docs.rubrik.com/en-us/saas/install/download_install_cdm_on_appliance_nodes.html.
28. Rubrik, "Setting up a Rubrik cluster using the UI", acceso el 20 de marzo de 2024, https://docs.rubrik.com/en-us/saas/install/setting_up_ui.html.
29. Rubrik, "Setting up a Rubrik cluster using the CLI", acceso el 20 de marzo de 2024, https://docs.rubrik.com/en-us/saas/install/setting_up_cli.html.
30. Rubrik, "Registering Rubrik clusters using the online method", acceso el 20 de marzo de 2024, https://docs.rubrik.com/en-us/saas/install/registering_clusters_online.html.
31. Rubrik, "Registering Rubrik clusters using the offline method", acceso el 2 de abril de 2024, https://docs.rubrik.com/en-us/saas/install/registering_clusters_offline.html.
32. Rubrik, "Enabling MFA", acceso el 21 de marzo de 2024, https://docs.rubrik.com/en-us/saas/install/rsc_enabling_mfa.html.
33. Rubrik, "Adding the initial account", 21 de marzo de 2024, https://docs.rubrik.com/en-us/saas/saas/adding_the_initial_account.html.
34. TrustRadius, "Learning Rubrik by putting the pieces together Brik by Brik", acceso el 21 de marzo de 2024, https://www.trustradius.com/reviews/rubrik-2023-09-20-21-03-04.
35. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".

36. Index Engines, "CyberSense®: How it Works", acceso el 21 de marzo de 2024, https://www.indexengines.com/how-it-works.
37. Rubrik, "Anomaly event details", acceso el 21 de marzo de 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_event_details.html.
38. Rubrik, "Events page", acceso el 21 de marzo de 2024, https://docs.rubrik.com/en-us/saas/saas/common/events_page.html.
39. Rubrik, "RSC Data Threat Analytics", acceso el 21 de marzo de 2024, https://docs.rubrik.com/en-us/saas/saas/ri_ransomware_monitoring.html.
40. Rubrik, "RSC Data Threat Analytics".
41. Dell Technologies, "Dell PowerProtect Cyber Recovery: Reference Architecture", acceso el 6 de mayo de 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h18661-dell-powerprotect-cyber-recovery-reference-architecture-wp.pdf.
42. Dell Technologies, "Dell EMC Avamar for Hyper-V", acceso el 16 de mayo de 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu89876.pdf.
43. Dell Technologies, "Dell EMC NetWorker Module for Microsoft for Hyper-V", acceso el 16 de mayo de 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu92011.pdf.
44. VMware, "Accelerate IT. Innovate with your cloud.", 9 de mayo de 2024, https://www.vmware.com/files/pdf/VMware-Corporate-Brochure-BR-EN.pdf.
45. Statista, "Cloud infrastructure services vendor market share worldwide from fourth quarter 2017 to first quarter 2024", 17 de julio de 2024, https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/.
46. Rubrik, "RSC Data Threat Analytics".
47. Dell Technologies, "CyberSense® for PowerProtect Cyber Recovery", acceso el 27 de junio de 2024, https://www.delltechnologies.com/asset/en-gb/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.
48. Rubrik, "RSC Data Threat Analytics".
49. Index Engines, "CyberSense® Support Matrix", acceso el 21 de marzo de 2024, https://www.indexengines.com/csmatrix.
50. Dell Technologies, "CyberSense® for PowerProtect Cyber Recovery".
51. Rubrik, "Keep Your Databases Running in the Face of Any Threat".
52. Index Engines, "CyberSense® Support Matrix".
53. Dell Technologies, "Dell EMC Avamar for Hyper-V".
54. Dell Technologies, "Dell EMC NetWorker Module for Microsoft for Hyper-V".
55. Rubrik, "Anomaly incidents", acceso el 2 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_incident.html.
56. Rubrik, "Data Threat Analytics Events", acceso el 2 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/ri_events.html.
57. Rubrik, "Viewing Anomaly Detection", acceso el 2 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/viewing_ri_investigations.html.
58. Rubrik, "VM Encryption Detection", acceso el 2 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/vm_encryption_detection.html.
59. Rubrik, "Viewing the Threat Monitoring page", 2 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/viewing_the_threat_monitoring_page.html.
60. Rubrik, "Iniciating a Threat Hunt", acceso el 2 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html.
61. Rubrik, "Quarantining matched files or objects", acceso el 2 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/quarantining_matched_objects_or_files.html.
62. Dell, "CyberSense® for PowerProtect Cyber Recovery".
63. Dell, "CyberSense® for PowerProtect Cyber Recovery".
64. Index Engines, "The Power of CyberSense's Machine Learning", acceso el 2 de abril de 2024, https://go.indexengines.com/csmachinelearning.
65. Index Engines, "The Power of CyberSense's Machine Learning".
66. Index Engines, "The Power of CyberSense's Machine Learning".
67. Dell, "CyberSense® for PowerProtect Cyber Recovery".
68. Rubrik, "Anomaly Detection behavioral model", acceso el 20 de mayo de 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_detection_behavioral_model.html.
69. Amazon, "Entrenamiento de modelos de ML", acceso el 2 de abril de 2024, https://docs.aws.amazon.com/es_es/machine-learning/latest/dg/training-ml-models.html.
70. Rubrik, "Defense in Depth with Polaris Radar", acceso el 21 de marzo de 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/Defense-In-Depth-Polaris-Radar-Technical-White-Paper.pdf.
71. Rubrik, "Data Threat Analytics dashboard", acceso el 21 de marzo de 2024, https://docs.rubrik.com/en-us/saas/saas/ri_dashboard.html.
72. Rubrik, "Initiating a threat hunt", acceso el 21 de marzo de 2024, https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html.
73. SentinelOne, "What Is A Malware File Signature (And How Does It Work)?", acceso el 4 de abril de 2024, https://www.sentinelone.com/blog/what-is-a-malware-file-signature-and-how-does-it-work/.

74. Rubrik, "Threat hunts", acceso el 21 de marzo de 2024, https://docs.rubrik.com/en-us/saas/saas/ri_threat_hunts.html.
75. Rubrik, "Anomaly Detection features", acceso el 22 de marzo de 2024, https://docs.rubrik.com/en-us/saas/saas/ri_features.html.
76. Rubrik, "Behavioral model".
77. Index Engines, "The Power of CyberSense's Machine Learning".
78. Dell, "CyberSense® for PowerProtect Cyber Recovery".
79. Rubrik, "Behavioral model".
80. Rubrik, "Anomaly Detection features".
81. Rubrik, "Behavioral model".
82. Dell, "CyberSense® for PowerProtect Cyber Recovery".
83. Morningstar, "Index Engines' CyberSense Announces 99.99% SLA in Detecting Ransomware Corruption, Empowering Smarter Recovery", acceso el 17 de julio de 2024, https://www.morningstar.com/news/pr-newswire/20240618ny41171/index-engines-cybersense-announces-9999-sla-in-detecting-ransomware-corruption-empowering-smarter-recovery.
84. Rubrik, "Threat Monitoring", acceso el 22 de marzo de 2024, https://docs.rubrik.com/en-us/saas/saas/threat_monitoring.html.
85. Index Engines, "The Power of CyberSense's Machine Learning".
86. Index Engines, "The Power of CyberSense's Machine Learning".
87. Rubrik, "Anomaly Detection features", acceso el 22 de marzo de 2024, https://docs.rubrik.com/en-us/saas/saas/ri_features.html.
88. Index Engines, "The Power of CyberSense's Machine Learning".
89. Rubrik, "Investigating and recovering anomalous files for filesets", acceso el 22 de marzo de 2024, https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files.html.
90. Rubrik, "Investigating and recovering anomalous files for virtual machines", acceso el 22 de marzo de 2024, https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files_for_virtual_machines.html.
91. Rubrik, "Full snapshot recovery of a virtual machine", acceso el 22 de marzo de 2024, https://docs.rubrik.com/en-us/saas/saas/full_snapshot_recovery_of_a_virtual_machine.html.
92. Rubrik, "Recovery of a batch of virtual machines", acceso el 22 de marzo de 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
93. Rubrik, "Performing bulk recovery for Recovery Plans", acceso el 22 de marzo de 2024, https://docs.rubrik.com/en-us/saas/saas/performing_bulk_recovery_for_recoveryplans.html.
94. Rubrik, "Recovery of a batch of virtual machines", acceso el 4 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
95. Rubrik, "Recovery of virtual machines", acceso el 16 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/vs_recovery_vm.html.
96. El almacén de datos recuperado suele estar en el clúster de Rubrik y no en el entorno de producción.
97. Rubrik, "Recovery of a batch of virtual machines", acceso el 16 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
98. Dell, "Restore plan", acceso el 16 de abril de 2024, https://infohub.delltechnologies.com/en-US/l/powerprotect-data-manager-protection-for-vmware-cloud-foundation-on-dell-emc-vxrail-1/restore-plan/.
99. Dell, "PowerProtect Data Manager Overview", acceso el 16 de abril de 2024, https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-manager-deployment-best-practices-1/powerprotect-data-manager-overview-4/.
100. Dell, "PowerProtect Data Manager 19.9 Administration and User Guide", acceso el 16 de abril de 2024, https://www.dell.com/support/manuals/en-us/enterprise-copy-data-management/pp-dm_19.9_ag/file-level-restore-of-a-powerprotect-backup-in-the-vsphere-client.
101. Dell, "Recovery Orchestration with PowerProtect Data Manager Overview", acceso el 16 de abril de 2024, https://www.youtube.com/watch?v=po2oMnAg_x4.
102. Rubrik, "Quarantine files or objects", 24 de marzo de 2024, https://docs.rubrik.com/en-us/saas/saas/quarantine.html.
103. Rubrik, "Downloading quarantined files for forensic analysis", 24 de marzo de 2024, https://docs.rubrik.com/en-us/saas/saas/downloading_quarantined_files_for_forensic_analysis.html.
104. Forrester, "The Total Economic Impact™ Of Dell PowerProtect Cyber Recovery", acceso el 16 de abril de 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/the-total-economic-impact-dell-powerprotect-cyber-recovery.pdf.
105. Rubrik, "Workload recovery during an RSC service disruption", acceso el 16 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/workload_recovery_during_rsc_outage.html.
106. Rubrik, "Rubrik CDM APIs and service account workflows", acceso el 16 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/rubrik_apis_sa_workflows.html.
107. Rubrik, "Recoverable workloads during RSC service disruption", acceso el 16 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html.
108. Rubrik, "Workloads require third-party tools for recovery", acceso el 16 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html.

109. NIST, "Computer Security Resource Center Glossary: air gap", acceso el 29 de julio de 2024, https://csrc.nist.gov/glossary/term/air_gap.

110. Dell, "Dell PowerProtect Cyber Recovery Solution Guide".

111. Dell, "Dell PowerProtect Cyber Recovery: Reference Architecture".

112. Adam Eckerle, "Debunking the Myths about Air Gaps", acceso el 14 de marzo de 2024, https://www.rubrik.com/blog/technology/2021/11/debunking-the-myths-about-air-gaps.

113. Rubrik, "Air-Gap, Isolated Recovery, and Ransomware - Cost vs. Value", acceso el 14 de marzo de 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/Air-Gap-Isolated-Recovery-and-Ransomware-Cost-vs.-Value.pdf.

114. Brian Williams, "Rubrik Air Gap and Inmutability", acceso el 14 de marzo de 2024, https://vimeo.com/561870246.

115. Rubrik, "Retention locks in the Rubrik cluster", acceso el 18 de marzo de 2024, https://docs.rubrik.com/en-us/9.0/sg/security_guide/retention_locks_in_the_rubrik_cluster.html.

Consulte la versión original en inglés de este informe

Este proyecto fue encargado por Dell Technologies.

Principled Technologies®

Facts matter.®