Commvault

GUÍA DEL COMPRADOR

Alineando la protección contra el ransomware y los planes de recuperación con las capacidades críticas

La empresa en evolución y la amenaza del ransomware

Las organizaciones se enfrentan a un entorno de datos cada vez más turbulento debido a una serie de factores que van desde el aumento de los empleos híbridos y remotos a la creciente expansión de los datos y el aumento de las ciberamenazas avanzadas. Se prevé que los daños causados por el cibercrimen alcancen los 10,5 billones de dólares anuales en 2025.[1] Las empresas necesitan soluciones de vanguardia que vayan más allá de las aplicaciones tradicionales de backup y recuperación para alcanzar una auténtica ciberresiliencia en el mundo híbrido. Estas soluciones permiten a las empresas no sólo proteger sus datos, sino también adelantarse de forma proactiva a los riesgos potenciales, minimizar los daños y recuperarse con rapidez ante la adversidad. A su vez, ello ayuda a las organizaciones a reducir la exposición general al riesgo y gestionar los costes de manera efectiva.

$10.5 BILLONES
anuales en 2025.[1]

Es obvio que las viejas costumbres ya no son efectivas. Las organizaciones están avanzando hacia una nueva generación de soluciones de seguridad basadas en marcos multicapa que aportan defensas activas, así como hacia una automatización que ofrezca el mejor plan de acción para protegerse contra los ataques de ransomware y recuperarse de ellos.

PROPÓSITO DE ESTA GUÍA

Utilice esta guía para evaluar sus capacidades actuales de protección y recuperación contra el ransomware y determinar el mejor modo de optimizar su plan de preparación en entornos de cargas de trabajo híbridas, de nube o SaaS.

1 Cybersecurity Ventures, Steven C. Morgan, Cybercrime to Cost The World 8 Trillion Annually In 2023, octubre de 2022

El marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST)

01 **IDENTIFICAR:** Desarrollar un proceso de comprensión sobre la organización para gestionar los riesgos de ciberseguridad en sistemas, personas, activos, datos y capacidades.

02 **PROTEGER:** Garantizar la prestación de servicios críticos mediante el desarrollo y la implementación de las defensas adecuadas.

03 **SUPERVISAR:** Establecer procedimientos continuos para identificar la aparición de eventos de ciberseguridad.

04 **RESPONDER:** Implementar las acciones adecuadas para defenderse contra incidentes de ciberseguridad conocidos.

05 **RECUPERAR:** Desarrollar e implementar las acciones adecuadas para mantener planes de resiliencia y restaurar cualquier capacidad o servicio que se vea afectado por un incidente de ciberseguridad.

Para ayudar a fortalecer la resiliencia de sus infraestructuras de datos, el actual Marco de ciberseguridad del NIST V1.1 recomienda cinco pilares principales de cara a contar con un programa de ciberseguridad integral y con garantías.

Para gestionar eficazmente los riesgos de ciberseguridad en un entorno siempre cambiante, el NIST ha elaborado una versión actualizada del marco: CSF 2.0. Esta versión actualizada, que se lanzará a principios de 2024, introduce un sexto pilar, Gobierno, que reposiciona los componentes de gobernanza dentro de los cinco pilares existentes y hace hincapié en la ciberseguridad como fuente importante de riesgo empresarial.

En cada sección de esta guía mostramos por qué cada capa de seguridad es esencial y revisamos las capacidades clave a integrar en su solución de protección y recuperación contra el ransomware.

01 IDENTIFICAR

En un mundo híbrido, saber exactamente dónde y cómo se utilizan los datos críticos no es un reto menor. Las herramientas de seguridad de datos eficaces deben proporcionar visibilidad en todo su entorno de datos para identificar mejor las áreas de riesgo y eliminar los puntos ciegos. Protegen tanto los datos como las copias de seguridad con una arquitectura de confianza cero que incluye protocolos de seguridad integrados para proteger los datos, evitar el acceso no deseado e impulsar el cumplimiento ante la evolución de las ciberamenazas. En caso de que el ataque tenga éxito, la visibilidad de extremo a extremo ayuda a las organizaciones a tomar mejores decisiones sobre sus datos antes, durante y después del mismo.

IDENTIFICAR COMPONENTES CLAVE	REQUISITOS CONTRA EL RANSOMWARE	CAPACIDADES DE COMMVAULT
Información sobre protección de datos	Análisis e identificación automáticos de problemas con acciones recomendadas para abordar consideraciones de seguridad.	Alertas, resúmenes y recomendaciones en tiempo real basados en IA dentro de Commvault® Cloud.
Evaluación de seguridad automatizada	Emplee conjuntos de herramientas interactivas para evaluar rápidamente la postura de seguridad y aplicar recomendaciones de cara a su mejora.	Tome medidas proactivas antes de que los ataques causen daños o se propaguen mediante paneles de control integrales que brindan información detallada sobre todos los aspectos de la seguridad de los datos.
Evaluación automatizada del estado del backup	Verifique que las copias de seguridad están en buen estado.	Las métricas «on-premise» y en la nube proporcionan informes de estado periódicos.
Informes y paneles de gestión de datos	Visualice rápidamente su estado de preparación para el backup y la recuperación. Con informes y paneles de control personalizados para elementos de interés específicos.	Los paneles unificados y los informes extensibles ofrecen preparación para la recuperación con indicadores de rendimiento (KPI) detallados.
Auditoría	Seguimiento de cambios en los datos, incluyendo quién accedió a ellos y cuándo se cambiaron.	Audite inicios de sesión vinculados a usuarios y direcciones IP específicos. Supervise todos los cambios de configuración y los eventos de backup y restauración mediante registros de auditoría detallados.
Tecnologías de engaño	Intercepte los ataques antes de que alcancen sus objetivos.	Threatwise™ proporciona herramientas diferenciadas para detectar amenazas desconocidas y de día cero en entornos de producción, lo que ayuda a los clientes a identificar ciberamenazas avanzadas antes de que los datos peligren.
Análisis de riesgo	Identifique e investigue datos confidenciales y en riesgo para minimizar su exposición y exfiltración.	• Identifique, categorice y clasifique información confidencial, como datos personales y financieros, para priorizar las medidas de seguridad y reducir la filtración de datos en caso de brecha. • Tome medidas proactivas para garantizar el cumplimiento normativo y ahorrar costes de almacenamiento mediante el archivo de los datos obsoletos (ROT). • Safe Search & Share utiliza la IA para identificar rápidamente datos y relaciones confidenciales dentro de grandes conjuntos de datos, garantizando que solo se comparte la información correcta con las personas adecuadas.
Threat Scan	Identifique e investigue anomalías en los archivos para asegurarse de recuperar datos en buen estado y evitar la reinfección con malware.	• Identifique amenazas de malware para evitar reinfecciones durante la recuperación. • Threat Scan analiza los datos de backup para localizar archivos cifrados o corruptos, lo que garantiza que los usuarios recuperarán rápidamente versiones fiables de sus datos. • Threat Scan Predict añade tecnología predictiva de IA en tiempo real para descubrir amenazas de ransomware basadas en esta tecnología.

02 PROTEGER

Gracias a la comprensión de su entorno de datos, usted podrá empezar a reducir su superficie de ataque para limitar las amenazas potenciales y evitar la propagación sistémica. Prevenga el acceso no deseado protegiéndose contra cambios en los datos desde dentro y desde fuera con una arquitectura de confianza cero. Podrá aislar y segmentar redes, adoptar espacios de «air-gapping» para aislar y proteger las copias de backup e incorporar tecnologías de engaño para interceptar amenazas antes de que se produzca la filtración, cifrado o exfiltración de los datos. Los ataques de ransomware pueden producirse cuando las credenciales se ven comprometidas o permiten a usuarios no autorizados un acceso privilegiado a los sistemas que nunca debería haber tenido. Asegúrese de que existen protocolos de seguridad normalizados para cifrar y proteger los datos a fin de reducir el impacto de los ataques de ransomware.

PROTEGER COMPONENTES CLAVE	REQUISITOS CONTRA EL RANSOMWARE	CAPACIDADES DE COMMVAULT
Inmutabilidad	Mantenga los datos de backup a salvo de cambios no autorizados.	• Protección anti-ransomware para sistemas basados en Windows y Linux. • Aplique bloqueos de almacenamiento tanto «on-premise» como en la nube, personalizando en función de las necesidades de su negocio. • Habilite WORM (Write Once, Read Many) para evitar cambios no autorizados y tecnología de air-gapping en la nube para incrementar la protección contra amenazas de ransomware.
Fortificación de infraestructuras	Reduzca la exposición ante amenazas de la infraestructura de backup.	El software de Commvault® ha sido probado y verificado como hábil para fortificación («hardening») de Nivel 1 por el por el Centro para la Seguridad de Internet (CIS). El cumplimiento de los controles CIS de Nivel 1 está disponible como VM reforzada (implementada a través de OVA) o como «appliance» de hardware (HyperScale X™). Todos los subcomponentes, incluyendo CommServe, agentes y nodos de acceso, pueden fortificarse también hasta CIS de Nivel 1.
Autenticación y autorización	Controle quién tiene acceso y qué nivel de acceso tiene mientras agrega múltiples capas de autorización para ampliar la seguridad.	• Los controles de acceso basados en roles limitan el uso no autorizado trabajando con sistemas SAML (Security Assertion Markup Language) y OATH IdP para proporcionar una capa adicional de seguridad. • Integración con Active Directory y LDAP. • Controles de autenticación multifactor y multipersona para bloqueos de retención y autorización de comandos para proteger los datos contra accidentes y evitar acciones destructivas. • Integración con gestión de acceso privilegiado y herramientas mejoradas de gestión de accesos e identidades como CyberArk, Yubikey y biometría para mayor autenticación y seguridad de los usuarios (AAL3). • Integración «Just-In-Time» con CyberArk para minimizar el riesgo de acceso a las credenciales almacenadas • Cifrado de datos de extremo a extremo al tiempo que se permite la gestión de claves y la autenticación de certificadosa desde plataformas externas para proteger contra el acceso malicioso a los datos. • WORM por software (bloqueo de retención) • «Multitenancy»

02 PROTEGER

PROTEGER COMPONENTES CLAVE	REQUISITOS CONTRA EL RANSOMWARE	CAPACIDADES DE COMMVAULT
Cifrado	Implemente estándares de cifrado que cumplan con las directrices del sector.	Estándares y herramientas para gestionar eficazmente las claves de cifrado de copias de seguridad y restauración en Commvault: • Módulo de cifrado FIPS (Federal Information Processing Standards) • Gestión de claves integrada • Integración con gestión de claves de terceros • Frase clave de KMS (Key Management System)
Protección del catálogo de backup	Garantice una protección inmutable en múltiples áreas, ya sean copias locales «on-premise» o en la nube.	• Protección anti-ransomware avanzada para copias locales. • Backup a Air Gap Protect o a una nube de terceros.
Aislamiento/ «air-gapping»	Segmente y aísle los datos de las redes externas y garantice una recuperación rápida en caso de ataque.	• Air Gap Protect utiliza tecnología de «air-gapping» aire para aislar y proteger datos confidenciales. • Los «appliances» HyperScale X cuentan con controles «air gap» integrados. • Topologías de red: utilice topología unidireccional o proxy.
Protección de Active Directory	Cree la capacidad de proteger y restaurar Active Directory, haga backup de atributos de objetos y realice backups completos, diferenciales, incrementales y sintéticos.	• La plataforma Commvault Cloud ofrece protección de Active Directory «on-prem» o en la nube con «air-gapping».
Estrategia de copia de seguridad 3-2-1	Cree una estrategia de backup efectiva que garantice que los datos estarán siempre disponibles. Cuente con al menos tres copias de los datos, dos de ellas locales pero en diferentes ubicaciones y otra fuera de las instalaciones.	• Configure copias ilimitadas de datos «on-prem» o en múltiples «endpoints» en la nube. • Air Gap Protect permite habilitar almacenamiento en la nube con «air-gapping».
Tecnologías de engaño	Detecte los ataques de ransomware con antelación, antes de que se produzcan fugas, cifrado, exfiltración o daños de datos.	• Abarque toda la superficie de ataque mediante el despliegue masivo de sensores de amenazas (falsos señuelos). • Imite activos críticos con sensores preconfigurados. • Emule activos altamente especializados exclusivos de su entorno.
Controles de seguridad bajo demanda	Garantice el control y el cumplimiento con políticas de rotación de contraseñas que no afecten a la protección de las copias de seguridad.	Mejore la postura de seguridad con control de confianza cero y elimine las credenciales comprometidas. La integración de CyberArk permite la recuperación de credenciales en modo «Just-In-Time», incluyendo el almacenamiento y la gestión segura de credenciales dentro de la propia aplicación.

03 SUPERVISAR

Es posible que las organizaciones afectadas por una amenaza de seguridad ni siquiera sepan que han sido atacadas hasta que ya es demasiado tarde y la brecha se ha propagado más allá de su control. Por ello, asegurar la implementación de herramientas adecuadas que permitan obtener rápidamente información sobre cualquier evento de ciberseguridad será esencial para contener el ataque antes de que se propagye a lo largo de la infraestructura. La incorporación de sistemas de alerta temprana y supervisión profunda de última generación permite descubrir y neutralizar amenazas internas y de día cero para defender sus datos. Detecte, desvíe y marque actividades maliciosas con mayor antelación para reducir los esfuerzos de recuperación.

SUPERVISAR COMPONENTES CLAVE	REQUISITOS CONTRA EL RANSOMWARE	CAPACIDADES DE COMMVAULT
Supervisión de seguridad con IA	Utilice IA para supervisar anomalías en backups de VMs y aplicaciones SaaS para obtener una visibilidad granular de actividad inusual en los archivos mediante auditorías para identificar potenciales eventos de seguridad.	Saque partido al potencial de la IA para: • Lograr una recuperación limpia, rápida y segura al tiempo que reduce los falsos positivos con IA y aprendizaje automático. • Supervisar las copias de seguridad y analizar eventos y comportamientos para definir si su estado es «completado», «pendiente» o «fallido». • Predecir el cumplimiento futuro de los acuerdos SLA mediante el análisis de tendencias de backup.
Supervisión del sistema	Supervisión de cargas de trabajo e infraestructuras críticas.	• Identifique anomalías por cambios de características de los archivos debidas a corrupción, cifrado o archivos maliciosos, tanto en datos activos como de backup. • Descubra nuevas amenazas de ransomware de día cero impulsadas por IA.
Monitorización de logs	Localice eventos log específicos para monitorizar la actividad en su entorno. Busque eventos concretos entre todos los eventos log indexados en el panel de control. Busque eventos log asociados a clientes, ficheros log, plantillas o políticas en particular.	La plataforma Commvault Cloud le permite supervisar las condiciones de los ficheros log y los eventos de Syslog y Windows con detalle de nivel granular.
Detección de amenazas	Obtenga de forma proactiva información inmediata sobre amenazas activas y latentes.	• Exponga los sensores únicamente a los atacantes, de modo que sean invisibles para usuarios y sistemas legítimos. • Obtenga información crítica sobre actividades y tácticas. • Elimine falsos positivos y la “fatiga de alertas”. • Atraiga a los atacantes para que utilicen recursos falsos.

03 SUPERVISAR

SUPERVISAR COMPONENTES CLAVE	REQUISITOS CONTRA EL RANSOMWARE	CAPACIDADES DE COMMVAULT
Cebos y actividad de archivos en vivo	Supervise los activos en riesgo de ransomware e identifique puntos de recuperación limpios.	Supervise archivos sospechosos en vivo para detectar amenazas y proteger las copias de seguridad a fin de garantizar una recuperación limpia de los archivos y evitar su reinfección.
Detección de amenazas	Obtenga de forma proactiva información inmediata sobre amenazas activas y latentes.	• Exponga los sensores únicamente a los atacantes, de modo que sean invisibles para usuarios y sistemas legítimos. • Obtenga información crítica sobre actividades y tácticas. • Elimine falsos positivos y la "fatiga de alertas". • Atraiga a los atacantes para que utilicen recursos falsos.
Supervisión de seguridad con IA	Utilice inteligencia artificial para supervisar marcos de anomalía en backups de VMs y otras cargas de trabajo como aplicaciones SaaS.	• Obtenga información cada vez que se produzcan cambios anormales en los backups para impulsar una recuperación limpia, rápida y segura. • Encuentre versiones limpias de datos para impulsar una recuperación limpia, rápida y segura. • Reduzca los falsos positivos con AI y aprendizaje automático ("Machine Learning").
«Honeypots» y actividad de archivos en vivo	Supervise los activos en riesgo de ransomware e identifique puntos de recuperación limpios.	Supervise archivos sospechosos en vivo para detectar amenazas y proteger las copias de seguridad a fin de garantizar una recuperación limpia de los archivos y evitar su reinfección.

04 RESPONDER

Una vez que se detecta ransomware, la respuesta debe ser inmediata. Obtener información a través de herramientas de seguridad y alertas proactivas le permitirá defender los datos de su organización. Contar con políticas documentadas y un plan de respuesta ante incidentes ayudará a determinar los pasos siguientes. Debe haber una respuesta tanto técnica como de negocio, y todos los actores, en cada una de sus respectivas áreas, deberán comprender su rol y las acciones que han de seguir. La coordinación y comunicación entre equipos es fundamental. La clave es conseguir que los equipos de seguridad hagan todo lo posible por contener y detener la propagación, al tiempo que se implementan las herramientas adecuadas para evitar cualquier posible reinfección.

RESPONDER COMPONENTES CLAVE	REQUISITOS CONTRA EL RANSOMWARE	CAPACIDADES DE COMMVAULT
Integración de SIEM (gestión de información y eventos de seguridad) y SOAR (orquestación, automatización y respuesta de seguridad)	Será necesaria una integración perfecta con las plataformas SIEM y SOAR existentes que permita supervisar, gestionar y orquestar acciones y eventos desde una ubicación central. Exporte eventos y notas de auditoría y regístrelos de forma segura en sus plataformas SIEM y SOAR con fines de preservación y orquestación de eventos. La monitorización en tiempo real permite responder rápidamente ante cualquier amenaza que se detecte y proteger los activos de backup con las acciones adecuadas.	Las integraciones de Commvault permiten la interoperabilidad con varias plataformas de orquestación como Microsoft Sentinel, Palo Alto Networks XSOAR, Splunk y ServiceNow. Nuestras integraciones proporcionan: • Visibilidad en tiempo real de eventos e incidentes de seguridad. • Capacidades mejoradas de automatización y orquestación. • Reducción de los tiempos de respuesta ante incidentes y de la intervención manual. • Mejoras en la colaboración interna y en la postura general de seguridad.
Alertas	Habilite notificaciones automáticas sobre operaciones (por ejemplo, tareas fallidas). Las alertas se muestran en la página «Triggered Alerts». Los usuarios definidos recibirán las notificaciones por correo electrónico.	Obtenga alertas procesables en diversos formatos: correo electrónico, SCOM (System Center Operations Manager), SNMP y webhooks, etc.
Paneles de control	Acceda a una vista previa de la información más crítica recopilada desde todos los sistemas CommServe de la organización, como porcentaje de cumplimiento SLA, uso de la capacidad e intentos de ataque a backups.	La plataforma Commvault Cloud proporciona un método unificado para visualizar y controlar la ciberresiliencia tanto «on-premise» como en SaaS. Ofrece paneles de control de seguridad, capacidad y uso a nivel global, con paneles de evaluaciones del estado de seguridad y actividad de archivos inusual que brindan información adicional.
Herramientas de orquestación	Cree flujos de trabajo orquestados para responder rápidamente ante eventos de ransomware. Incluso puede integrarlos con proveedores externos.	• Cree sencillamente flujos de trabajo para comandos pre- y post-backup. • Flujos de trabajo vía interfaz de línea de comandos, API REST, módulos PowerShell o el SDK para Python. • Intégrelos con Splunk, ServiceNow, Ansible o Terraform.
Respuesta proactiva ante amenazas	Defienda activamente la recuperabilidad de los datos alertando al equipo de seguridad en el momento en que el atacante empieza a actuar.	• Implemente sensores de amenazas en torno a los activos valiosos (como servidores de archivos, bases de datos, máquinas virtuales, etc.) para crear señuelos dentro de sus entornos. • El sistema recomienda de forma inteligente la mejor ubicación para los señuelos estudiando las cargas de trabajo en los entornos de backup. • Reciba alertas de alta precisión en el momento en que comienza un ataque.

05 RECUPERAR

El proceso de recuperación comienza una vez que se identifican las amenazas y una respuesta adecuada al incidente aísla y elimina el malware. Es fundamental garantizar que todos los datos afectados se restablezcan a las condiciones operativas normales desde el momento previo al incidente de ciberseguridad. Es un hecho probado que las herramientas y opciones de recuperación proactivas y fiables con una amplia cobertura para cargas de trabajo reducen el tiempo de inactividad, impiden la pérdida de datos y aceleran los tiempos de respuesta para conseguir una continuidad de negocio sin comparación. El plan de recuperación comienza después de que se identifica la causa raíz y se restauran los archivos con la intención para que las herramientas de seguridad adecuadas mitiguen cualquier impacto potencial futuro. Durante las fases de recuperación, es esencial recuperar únicamente archivos limpios de todas las tecnologías afectadas.

RECUPERAR COMPONENTES CLAVE	REQUISITOS CONTRA EL RANSOMWARE	CAPACIDADES DE COMMVAULT
Recuperación en entornos híbridos «multi-cloud»	Recupere datos rápidamente desde cualquier lugar, ya sea «on-premise» o en la nube.	Automatice y recupere en diferentes hipervisores, hiperescalares u otras plataformas.
Alta disponibilidad	Con la función CommServe LiveSync, mantenga el servidor CommServe listo para la recuperación ante desastres y cuente con la capacidad de hacer rápidamente "fail-over" a un host de reserva designado para casos de desastre.	La función Commvault LiveSync permite realizar copias de seguridad de catálogos y otras cargas de trabajo críticas.
Recuperación para equipos de respuesta ante incidentes	Permita a los equipos de respuesta ante incidentes recuperar de forma segura datos para análisis periciales.	• Orqueste recuperaciones «out-of-place» en un entorno limpio y aislado. • Ejecute scripts y flujos de trabajo previos y posteriores para validar y escanear datos clave.
Escaneo de malware	Verifique que los datos de backup son recuperables y que no hay amenazas en los contenidos.	• Monte en vivo máquinas virtuales mediante la validación de aplicaciones para ejecutar scripts de forma segura y escanear máquinas virtuales en busca de malware. • Busque amenazas antes de que se propaguen con IA/aprendizaje automático, detección de anomalías y escaneo de firmas de malware.
Recuperación y desinfección	Reduzca la pérdida de datos mediante una recuperación consistente y limpia, eliminando archivos sospechosos y conociendo el momento exacto a partir del cual lograr una recuperación saludable de los archivos.	Elimine, aísle y ponga en cuarentena archivos sospechosos mediante la detección de anomalías y desinfecte el contenido de las copias de seguridad explorando y eliminando amenazas.

05 RECUPERAR

RECUPERAR COMPONENTES CLAVE	REQUISITOS CONTRA EL RANSOMWARE	CAPACIDADES DE COMMVAULT
Recuperación proactiva	Descubra y solucione las amenazas antes de que alcancen su objetivo.	Con Threatwise™, engañe a los atacantes, desvíe sus ataques hacia activos falsos, obtenga visibilidad inmediata de los ataques y solucione las amenazas en primera instancia, antes de que lleguen a sus datos.
Validación de recuperación	Planifique, implemente, valide y exhiba pruebas fehacientes de preparación para la recuperación.	• Valide los backups de forma continua o periódica para detectar copias de seguridad deterioradas en las primeras etapas del ciclo. • Pruebe y demuestre la preparación para la recuperación sin interrumpir las operaciones. • Reduzca la complejidad de las pruebas de recuperación con la eliminación de los pasos manuales.
Análisis forense de la recuperación	Realice análisis forense de forma segura en redes aisladas sin causar más infecciones.	• Utilice el análisis de datos de archivos para detectar archivos que puedan estar cifrados o dañados por malware y asegurarse de que no esté haciendo backup de archivos infectados. • Incorpore análisis de amenazas para detectar contenido malicioso en los datos respaldados en el momento de la restauración, a fin de garantizar que no corre el riesgo de reinfectar los sistemas de producción mientras realiza la restauración desde el último momento adecuado de las copias de seguridad.
Orquestación de la recuperación	Orquestación de ciberrecuperación y recuperación ante desastres con informes automatizados sobre cumplimiento.	• Recupere copias limpias con un solo clic en cargas de trabajo para producción una vez validados y desinfectados los puntos de recuperación.
Recuperación rápida de infraestructuras	Recuperación rápida a gran escala en la nube, sin limitaciones en las ubicaciones de recuperación.	• Combina pruebas continuas, infraestructura como código y escalado en la nube para automatizar una ciberrecuperación rápida, predecible y fiable de cargas de trabajo híbridas en la nube, con el coste total de propiedad (TCO) más bajo. • Portabilidad entre cualquier soporte que permite la recuperación desde y a cualquier lugar.

Auténtica ciberresiliencia con el TCO más bajo.

Commvault Cloud proporciona defensa en capas, minimizando el impacto de los ciberataques con alerta temprana y ciberengaño, al tiempo que acelera la recuperación con escaneo integral de amenazas, cuarentena inteligente, validación de recuperación limpia y velocidades de recuperación sin comparación.

Impulse su estrategia de ciberresiliencia con la mejor solución para ayudar a predecir, combatir proactivamente y acelerar la recuperación ante ciberamenazas.

Encuentre la mejor solución para sus necesidades.

INTEGRACIONES DE SEGURIDAD DE COMMVAULT

Commvault ofrece integraciones perfectas con los principales partners de seguridad para aprovechar mejor sus capacidades y ofrecer opciones variadas de ciberresiliencia en un entorno híbrido integrado.

Más información sobre la ciberresiliencia
commvault.com/es/plataforma

Commvault®

commvault.com | 91 078 14 56 | info-iberia@commvault.com