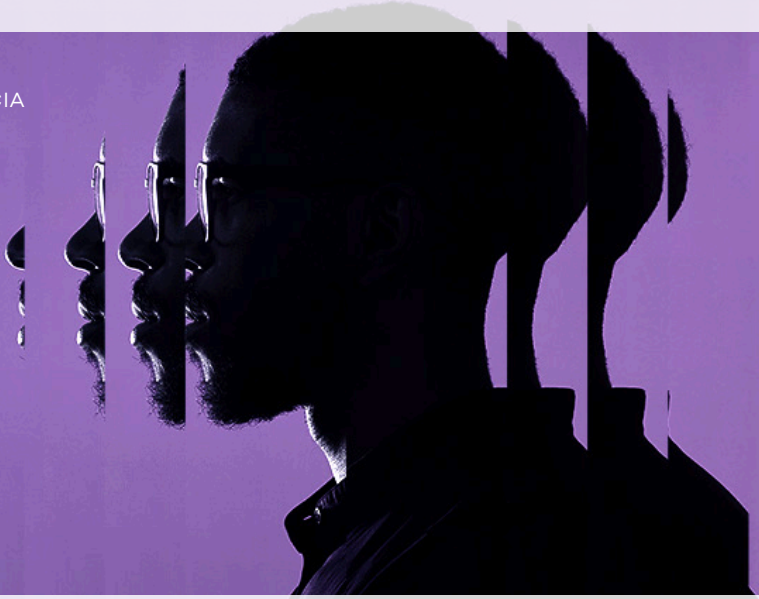
MANUAL DE CIBERRESILIENCIA

Mejores prácticas para pasar de la viabilidad mínima a la **ciberrecuperación completa**

Commvault®



VISIÓN GENERAL

Estar preparado para la ciberrecuperación es crucial en la era digital actual, donde las amenazas cibernéticas son cada vez más sofisticadas y omnipresentes.

Las estrategias de ciberrecuperación efectivas son fundamentales para combatir esas amenazas y permitir que tu negocio restaure rápidamente los sistemas y datos críticos después de un incidente cibernético, minimizando el tiempo de inactividad y mitigando el impacto en las operaciones del negocio.

Al estar preparadas cibernéticamente, las empresas demuestran a clientes, partes interesadas y organismos reguladores que se toman en serio la protección de datos sensibles y de los sistemas, y que cumplen con sus compromisos con los clientes.

El primer paso para construir un plan de preparación cibernética es identificar a las personas, procesos, sistemas y datos críticos necesarios para operar—esto es tu viabilidad mínima. Para la mayoría de las empresas, esto incluye la gestión ejecutiva y operativa, una comprensión de los roles y responsabilidades durante la recuperación, así como la capacidad técnica para restaurar sistemas críticos, como la identidad empresarial (por ejemplo, Active Directory), canales de comunicación (por ejemplo, correo electrónico, chat, herramientas de colaboración), y preparar y validar que los datos, aplicaciones e infraestructura estén limpios y listos para ser recuperados y restaurados desde la copia de seguridad. Más allá de los mandatos de cumplimiento (como GDPR, HIPAA, DORA o SOCI) que requieren planes detallados de ciberseguridad, resiliencia, recuperación ante desastres y continuidad del negocio, un plan de ciberrecuperación bien estructurado reduce el riesgo de pérdida de datos, asegurando que la información crítica, como los datos de los clientes, los datos de la organización y la propiedad intelectual, permanezcan protegidos. En caso de compromiso de datos, contar con un mecanismo de recuperación rápida ayuda a restaurar rápidamente las operaciones mínimas viables y a poner los sistemas de nuevo en línea rápidamente.

EL INFORME DE COMMVAULT + GIGAOM SUBRAYA LA NECESIDAD CRÍTICA DE ESTRATEGIAS DE CIBERRECUPERACIÓN COMPLETAS

Sigue leyendo para conocer los componentes esenciales necesarios para estar preparado para un ciberataque y mira cómo Commvault® Cloud proporciona las herramientas para ayudarte a tener éxito.

PASO #01

IDENTIFICAR

Un principio clave de cualquier estrategia es tener una visibilidad profunda del entorno y comprender qué aplicaciones, sistemas y datos son necesarios para garantizar la viabilidad mínima en caso de interrupciones y ciberataques..

Con Commvault Cloud, esto incluye la capacidad de descubrir, clasificar y monitorizar datos sensibles en todos tus repositorios de datos. La clasificación de los datos puede desencadenar políticas de protección y ayudar a guiar a las organizaciones hacia lo que es más crítico y lo que requiere un nivel diferente de protección.

Una vez que conoces los elementos que deben ser protegidos, puedes instrumentar el entorno con mecanismos de detección de amenazas, detección de anomalías y sistemas de alerta temprana para notificar a los equipos de seguridad sobre las amenazas en tus redes antes de que causen daño.

También necesitas un enfoque en capas cuando se trata de encontrar y detener malware, ransomware y otros vectores de corrupción de datos. Los datos deben ser inspeccionados en todos los puntos de su ciclo de vida para identificar datos corruptos y poder restaurarlos a un punto limpio en el tiempo.

PRODUCTOS DE COMMVAULT CLOUD PARA AYUDAR A IDENTIFICAR AMENAZAS:

- Risk Analysis para el descubrimiento y control de datos sensibles
- Threatwise™ para la detección de amenazas y anomalías y alertas tempranas
- Threat Scan para identificar datos maliciosos o corruptos

CAPACIDADES DE LA PLATAFORMA COMMVAULT CLOUD:

- Validación Cleanpoint

PASO #02

PROTEGER

Para estar preparado para un ataque inevitable, debes proteger tus datos contra las acciones de atacantes, personal interno malintencionados y hasta contra malas configuraciones o interrupciones. Esta protección es multifacética y debe tener en cuenta los datos en sí, la identidad y las configuraciones.

Comenzando con los datos, la mejor práctica dicta que las organizaciones sigan la regla 3-2-1: tres copias de datos, en dos tipos de medios (o en dos plataformas diferentes), y una copia que sea imposible de modificar. Duplicar los datos para los primeros dos pasos es sencillo, pero el tercero es un poco más desafiante. Necesitas un mecanismo que haga los datos inmutables e indelebles para protegerlos de cambios o eliminaciones unilaterales. Esto es especialmente importante por dos razones: la mayoría del ransomware tiene mecanismos para alterar las copias de seguridad, y las amenazas internas son reales.

También debes validar que tu infraestructura (tanto en la nube como de backup) esté configurada según los principios de zero trust. Deben existir mecanismos que verifiquen las configuraciones y reporten y alerten sobre cambios o "desviaciones".

La autenticación también debe seguir los principios de zero trust y debe incluir la autorización multifactor y multipersona, dependiendo de los niveles de acceso y las acciones que se estén realizando.

Además, cualquier mecanismo que tengas implementado para validar la identidad, como Active Directory o Entra ID, también debe estar configurado, respaldado y monitorizado en caso de cambios como adiciones, eliminaciones o elevaciones de privilegios.

Cualquier dato, configuración o plano de control debe estar respaldado para permitir la restauración en caso de un incidente de seguridad, y las copias de seguridad deben estar aisladas y air-gapped para reducir la probabilidad de que los atacantes encuentren las copias de seguridad durante el reconocimiento o que sean eliminadas o encriptadas por malware o ransomware.

PRODUCTOS DE COMMVAULT CLOUD QUE TE AYUDAN A PROTEGER TUS DATOS:

- Backup and Recovery para cargas de trabajo en la nube, on-premises y SaaS
- Backup and Recovery de Active Directory para proteger Active Directory y Entra ID
- Air Gap Protect para almacenamiento inmutable, indeleble y desconectado
- Threat Scan para identificar y aislar datos maliciosos o corruptos

CAPACIDADES DE LA PLATAFORMA COMMVAULT CLOUD:

- Security IQ para la gestión de la postura de seguridad de tu entorno de backup
- Control de acceso basado en roles (RBAC) y autorización multipersona

PASO #03

RESPONDER

Ninguna tecnología te servirá de mucho si se utiliza de forma aislada. Por eso, Commvault Cloud se integra con software de gestión de información y eventos de seguridad (SIEM) y plataformas de orquestación, automatización y remediación de seguridad (SOAR).

Esto permite compartir contexto entre Commvault Cloud y otras herramientas de seguridad para detectar mejor los eventos de seguridad, los problemas de integridad de datos y las actividades anómalas.

Tanto si estás utilizando la plataforma Palo Alto Networks XSOAR, Splunk SIEM, Microsoft Sentinel u otra herramienta, la detección de amenazas y anomalías de Commvault Cloud es un multiplicador de fuerza para construir ciberresiliencia y mejorar la respuesta a incidentes.

Cuando Commvault Cloud encuentra archivos sospechosos o recibe una alerta de anomalía de una integración, ese archivo puede ser aislado automáticamente de tus datos de producción, mientras se envía una copia a un Sandbox para su detonación y análisis con el fin de determinar si es malicioso.

CAPACIDADES DE LA PLATAFORMA COMMVAULT CLOUD QUE TE AYUDAN A RESPONDER MÁS RÁPIDO A LAS AMENAZAS:

- Integraciones con el ecosistema de seguridad wincluyendo tecnologías SIEM y SOAR
- Integraciones de inteligencia de amenazas para una cobertura más amplia de amenazas
- Integraciones de Sandbox para permitir la inspección y detonación de archivos sospechosos

PASO #04

RECUPERAR

Cuando llega el momento de recuperar datos, ya sea de un desastre o un ciberataque, necesitas un plan que haya sido practicado y documentado; datos limpios y completos; flexibilidad en los objetivos de restauración; la capacidad de restaurar todo, desde los datos hasta la aplicación que los utiliza; y velocidad.

Cuando llega el momento de recuperar datos, ya sea de un desastre o un ciberataque, necesitas un plan que haya sido practicado y documentado; datos limpios y completos; flexibilidad en los objetivos de restauración; la capacidad de restaurar todo, desde los datos hasta la aplicación que los utiliza; y velocidad.

El peor momento para darte cuenta de que tu plan de recuperación no va a funcionar es cuando estás frente a un ataque. Realizar pruebas regulares de planes de recuperación mínimos viables y completos es crucial para saber que puedes recuperarte cuando sea necesario, y ayuda a los equipos que realizan la recuperación a conocer lo que se espera de ellos. Estas pruebas o prácticas del proceso de recuperación deben verificar la integridad de los datos y ser capaces de restaurar datos y reconstruir aplicaciones en un nuevo entorno.

La portabilidad es importante para las pruebas y la recuperación, ya que un ataque o una interrupción puede requerir que muevas cargas de trabajo completas a un nuevo y diferente entorno. Esto podría significar simplemente cambiar de cuenta o podría ser tan drástico como moverse de un entorno local a la nube, o a una nube diferente por completo, por lo que tu recuperación debe ser híbrida y flexible.

Ya hemos discutido la necesidad de escanear y monitorizar los datos en busca de anomalías, malware y otros defectos. Cuando llega el momento de restaurar, es importante hacer una última verificación de los datos para validar que estén limpios, listos para restaurar y no vayan a reinfectar tu entorno.

Finalmente, después de una recuperación, necesitarás mantener una copia de los datos y sistemas que fueron afectados por el ataque para ofrecerla a equipos de investigación y respuesta a incidentes de terceros, fuerzas del orden, aseguradoras cibernéticas u otras partes interesadas. Esta copia forense debe mantenerse separada de tu entorno de producción y preservarse tal como está para tus investigaciones. Esto puede ayudar en el desarme del malware, la identificación del atacante y la identificación de técnicas y procedimientos a tener en cuenta en el futuro.

PRODUCTOS DE COMMVAULT CLOUD QUE TE AYUDAN A RECUPERARTE:

- Cleanroom Recovery para pruebas de recuperación, validación y estudio forense
- Threat Scan para validar que los archivos que se están recuperando estén limpios y libres de malware, ransomware y corrupción
- Cloud Rewind para reconstruir aplicaciones en diferentes nubes, desde el código hasta los datos
- Active Directory Recovery para la continuidad de la identidad, incluso frente a un ciberataque

CAPACIDADES DE LA PLATAFORMA COMMVAULT CLOUD:

- Cloudburst Recovery para una recuperación rápida y a escala de la nube, disponible cuando la necesites
- Cleanpoint Validation para proporcionar un punto de tiempo conocido y limpio al que puedas restaurar

PASO #05

MONITORIZAR

Toda tu planificación y preparación solo funcionarán si has implementado en tu entorno herramientas que alerten a los equipos de operaciones de seguridad y TI sobre anomalías o incidentes en tu infraestructura

La monitorización de amenazas que se han infiltrado en tu organización y que intentan evadir la detección es crucial para minimizar el daño que pueden causar. Cuanto antes te des cuenta de su presencia, antes podrás expulsarlas y restaurar los datos afectados.

El desafío con la monitorización es que muchas herramientas cibernéticas desencadenan cientos o miles de alertas, generando mucho ruido por falsos positivos. Esto lleva a los equipos de operaciones de seguridad por caminos de investigación sin salida, causando agotamiento y fatiga por alertas, y restando tiempo a las investigaciones de amenazas reales. Ajustar los sistemas para que solo alerten sobre ataques reales es crucial para ayudar a los equipos a enfocarse y encontrar amenazas sauténticas.

Los datos de producción y backup deben ser monitorizados continuamente para detectar cambios, anomalías y malware con el fin de ayudar a detectar amenazas más rápidamente, minimizar el riesgo de infecciones adicionales y restaurar a datos conocidos y limpios. Esto incluye la capacidad de analizar los comportamientos de los archivos, no solo su contenido, para poder detectar ataques nunca vistos.

También puedes beneficiarte de consolidar toda la monitorización en una sola plataforma, en la mayoría de los casos, una herramienta SIEM o SOAR que es supervisada continuamente por personal de operaciones de seguridad y utilizada para coordinar investigaciones y respuestas.

PRODUCTOS DE COMMVAULT CLOUD QUE PERMITEN LA MONITORIZACIÓN CONTINUA:

- Threatwise™ • Threatwise para la detección de atacantes que realizan reconocimiento y trampas que proporcionan alertas de alta fidelidad de una brecha
- Threat Scan para el escaneo continuo de datos de copia de seguridad y archivos en busca de malware
- Threat Scan Predict para descubrir ataques de día cero o impulsados por IA que son polimórficos

CAPACIDADES DE LA PLATAFORMA COMMVAULT CLOUD:

- SIntegraciones con el ecosistema de seguridad para agregar aún mayores niveles de inteligencia de amenazas de proveedores de terceros party providers

RESUMEN

En resumen, es necesario ser consciente de los riesgos que tus datos presentan para tu organización.

01

Identifica lo que necesitas para la viabilidad mínima: los sistemas, aplicaciones y datos críticos para el funcionamiento de tu negocio.

02

Invierte en herramientas avanzadas de protección, detección y monitorización para mejorar la capacidad de tu organización de detectar y responder rápidamente a amenazas cibernéticas.

03

Desarrolla y mantén un plan de respuesta a incidentes actualizado, que defina roles, responsabilidades y procedimientos claros a seguir en caso de una brecha de seguridadof a breach.

04

Realiza pruebas completas para validar que has cubierto múltiples escenarios y que puedes recuperarte por completo.

05

Monitoriza tus sistemas y copias de seguridad para tener la confianza de que están limpios y listos cuando sean necesarios.

Para ver cómo Commvault Cloud puede apoyar el aspecto tecnológico de tu estrategia de preparación cibernética, **ponte en contacto con nuestros expertos.**