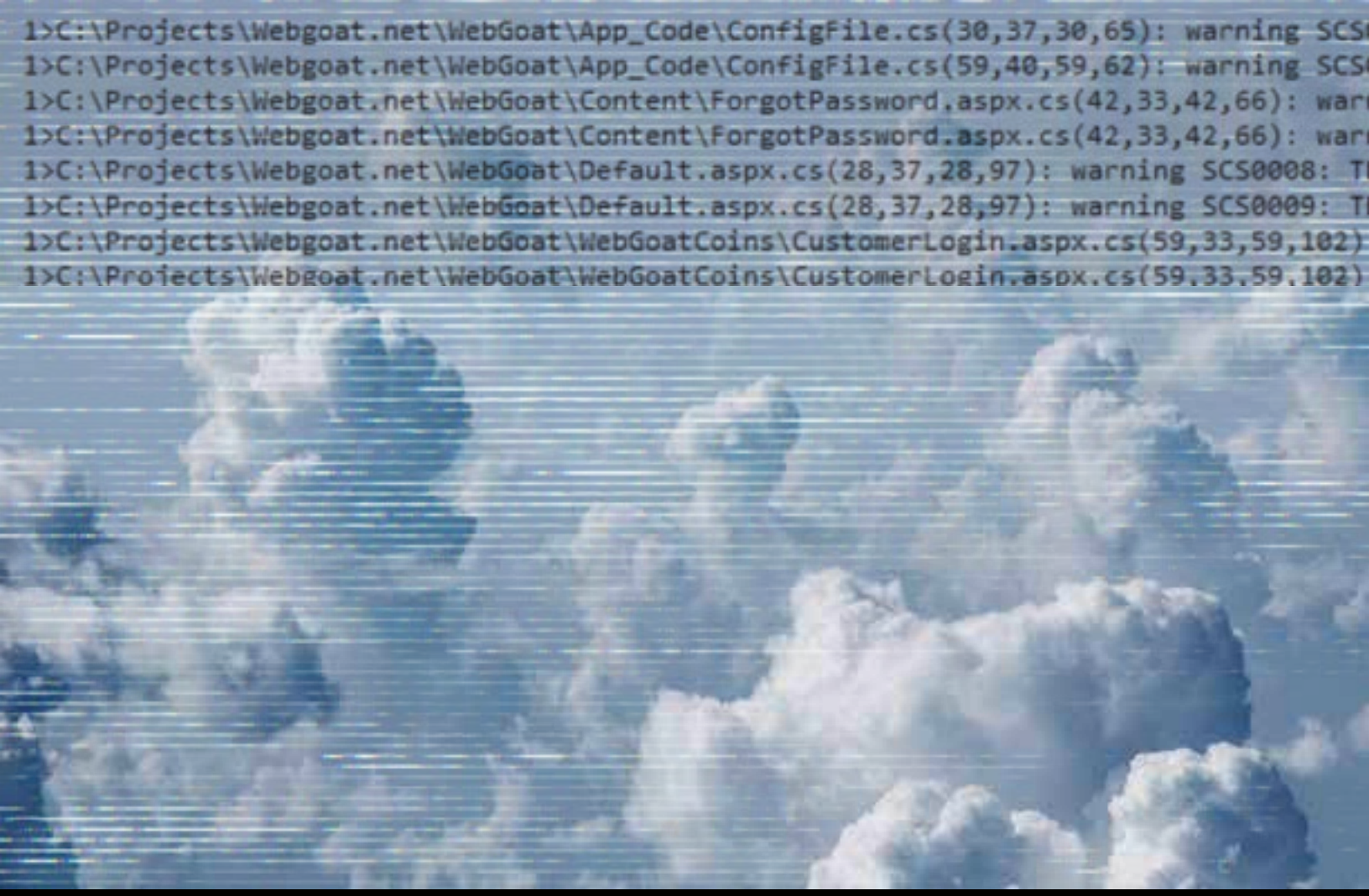

Guía

Commvault®

La solución de ransomware que le encantará a su responsable de seguridad

EL NUEVO PANORAMA DE AMENAZAS

En un panorama de amenazas en constante evolución como el actual, los ciberataques se han vuelto más generalizados y costosos que nunca. Para los responsables de seguridad y tecnología, desarrollar una estrategia sólida de ciberresiliencia y recuperación no sólo es esencial, sino urgente. La brechas **se producirán**. ¿Dispone su empresa de medios y recursos para detectar una brecha, y de un plan de respuesta para actuar?

Quizá confíe usted en soluciones de seguridad de datos tradicionales que recurren a un mosaico de soluciones mal integradas. En ese caso, sus equipos de seguridad estarán en desventaja desde el principio a la hora de identificar el alcance completo de los ataques.

Por otro lado, la falta de colaboración entre sus equipos de TI y seguridad durante el incidente hará que su organización quede aún más rezagada ante un adversario que se mueve con rapidez.

El precio de un plan de respuesta mal implementado es un tiempo de inactividad caro y prolongado, sanciones por incumplimiento, brechas de seguridad y, en última instancia, daños a la reputación de su organización.

365.000 $

es el coste del tiempo de inactividad por hora.[1]

EL CAOS EXIGE UN ENFOQUE UNIFICADO

Por desgracia, el caos y las horas de trabajo que siguen a una brecha de seguridad pueden dificultar la decisión de quién debe responder y cómo. No hay tiempo para conflictos internos. Los equipos de seguridad y TI deben trabajar codo con codo, tanto a nivel estratégico como táctico. Esta colaboración es vital para una gestión de riesgos eficiente y eficaz.

Sin embargo, solo el 30 % de los equipos de operaciones de seguridad comprenden completamente el rol de las operaciones de TI.

Y solo el 29 % de los equipos de TI entienden completamente las operaciones de seguridad.[2]

La ciberresiliencia puede servir como puente entre TI y Seguridad y reforzar la postura general de seguridad de la organización. Los líderes de ambos equipos deben dotar a su gente de las herramientas y estrategias adecuadas para mitigar los riesgos y proteger los datos y la reputación. Estas herramientas, además, deben integrarse para proporcionar contexto y una comprensión integral de los ataques, los incidentes y las brechas.

61%

de los CISO creen que su organización no está preparada para hacer frente a un ciberataque dirigido.[3]

Comience a construir una organización más ciberresiliente hoy, cerrando la brecha entre equipos de TI y seguridad. Prepárese para hacer frente a cualquier amenaza, incluido el ransomware, con una solución unificada que ofrece alertas tempranas, preparación para la recuperación continua y ciberrecuperación autoescalable. Opte por un abordaje que proteja los datos en toda su infraestructura de nube híbrida y facilite la recuperación tanto en entornos "on-premise" como de nube.

Por supuesto, el ransomware suele ser siempre síntoma de una brecha mayor, y sería torpe abordar solo el mecanismo de entrega del ransomware sin afrontar los problemas subyacentes para mitigar la brecha y erradicar el acceso de los atacantes. El hecho es que un 80 % de las empresas que sufrieron un ataque de ransomware tuvieron un segundo o tercer ataque. ¿Está su empresa preparada?

1 Splunk, "**Digital Resilience Pays Off Report**", febrero de 2023.
2 IDC, "**The Cyber-Resilient Organization: Maximum Preparedness with Bulletproof Recovery**", septiembre de 2023.
3 Proofpoint, "**2023 Voice of the CISO Report**", mayo de 2023.

TODOS ESTAMOS JUNTOS EN ESTO

Si bien el objetivo de todos los involucrados en la ciberresiliencia es proteger de daños a la empresa, puede que los equipos de TI y los de seguridad lo hagan de manera distinta, cosa que podría causar una exposición potencial a amenazas externas. La clave radica en establecer puntos en común. Estos son algunos ejemplos:

1. **Objetivos compartidos**: tanto los equipos de TI como los de seguridad tienen como objetivo proteger los activos, sistemas y datos de la organización. Trabajan para mantener la confidencialidad, integridad y disponibilidad de la información.

2. **Colaboración**: los equipos de TI y de seguridad suelen colaborar estrechamente para implementar y mantener medidas de seguridad. Trabajan juntos para identificar vulnerabilidades, implementar controles de seguridad y responder ante incidentes.

3. **Gestión de riesgos**: ambos equipos participan en la evaluación y gestión de riesgos. Los equipos de TI se centran en los riesgos operativos relacionados con la disponibilidad y el rendimiento del sistema, mientras que los equipos de seguridad trabajan para mitigar los riesgos asociados al acceso no autorizado, las brechas de datos y otros incidentes de seguridad.

4. **Cumplimiento**: los equipos de TI y seguridad trabajan juntos para garantizar el cumplimiento de las regulaciones y normas relevantes. Colaboran para implementar controles y procesos que cumplan con los requisitos legales y del sector.

5. **Respuesta ante incidentes**: en caso de un incidente de seguridad, los equipos de TI y de seguridad colaboran para investigar, contener y solucionar el problema. Trabajan juntos para minimizar el impacto y restaurar el funcionamiento normal.

6. **Sensibilización y formación**: ambos equipos desempeñan un papel en la promoción de la concienciación sobre la seguridad y la formación de los empleados. Los equipos de TI educan a los usuarios sobre prácticas informáticas seguras, mientras que los equipos de seguridad asesoran sobre el modo de identificar e informar de posibles amenazas a la seguridad.

7. **Pruebas de estrés**: un equipo que opera unido estrecha sus vínculos y consigue más resultados. Realice pruebas de estrés de sus planes, políticas y capacidad de interacción para detectar áreas de mejora potencial. Es mejor prepararlo todo en condiciones ideales que hacerlo bajo la tensión de un ataque.

En términos generales, la colaboración y comunicación efectiva entre los equipos de TI y de seguridad son cruciales para mantener una infraestructura de TI segura y resiliente.

LOS ATAQUES SUCEDEN. ASEGÚRESE DE QUE SUS EQUIPOS DE SEGURIDAD Y TI ESTÉN PREPARADOS.

Los directivos de TI y seguridad necesitan capacidades avanzadas de seguridad de datos para abordar los riesgos cibernéticos de manera efectiva, minimizar las amenazas y mejorar los resultados de la recuperación.

Recuerde que la cuestión no es **SI** se producirá una brecha, sino **CUÁNDO** la **DETECTARÁ**, **QUÉ** hizo para afrontarla y **CÓMO** responderá ante ella.

Iniciando la conversación

Para estimular una mejor colaboración y encontrar puntos en común, aquí tiene algunas cuestiones a tener presentes:

- ¿Cómo está de preparada su organización para responder ante las ciberamenazas y garantizar la continuidad del negocio en caso de incidente?
- ¿Cuáles son los activos críticos y cuál es el tiempo de inactividad esperado para el negocio?
- ¿Cuáles son las suposiciones que se han hecho sobre disponibilidad? ¿Se ha tenido en cuenta, por ejemplo, una posible caída de AD, o la interrupción de VMware, o la caída de alguna región de nube?
- ¿Entienden sus equipos los roles y las responsabilidades que tienen asignados durante un ataque?
- ¿Quién tiene acceso y visibilidad a qué? ¿Cuenta con mecanismos de conversación "off-band"?
- ¿Cómo protege y gestiona los datos al adoptar entornos de nube híbrida?
- ¿Cuánto le costaría a la empresa y a su reputación una brecha o un caso de ransomware?

COMMVAULT CLOUD: CIBERRESILIENCIA PARA EL MUNDO HÍBRIDO

También es imprescindible contar con la tecnología adecuada para cumplir esos objetivos comunes. Commvault Cloud®, con tecnología Metallic AI, es la única plataforma de ciberresiliencia creada para responder a las exigencias de la empresa híbrida y equipar a los equipos de operaciones de seguridad y TI con las capacidades de seguridad y recuperación de datos necesarias frente a la evolución de las amenazas con tecnología de IA.

En el mundo híbrido actual, ultracomplejo y en constante expansión, existen riesgos inherentes que resolver, mitigar y aceptar. ¿Podrá usted identificar rápidamente activos creados con poca o ningun aviso previo? ¿Conoce el software, el hardware y los servicios externos que podrían exponer sus datos a ciberamenazas? Todo esto obliga a los responsables de seguridad de la información a tomar decisiones difíciles sobre cómo priorizar y alinear de manera más efectiva recursos finitos, riesgos en constante expansión y necesidades de negocio.

Por muchas razones, las organizaciones buscan soluciones de un único proveedor. Las regulaciones, el cumplimiento y las políticas han empujado a las organizaciones a querer saber más sobre la ciberseguridad que ofrece el proveedor de servicios. Los responsables de TI y seguridad solicitan a los proveedores detalles sobre sus pruebas de penetración, ciclo de vida de desarrollo de software (SDLC), lista de materiales de software (SBOM) y otra documentación para demostrar que no heredarán una ciberseguridad deficiente.

Commvault Cloud se ha diseñado específicamente para proteger, supervisar, informar, gestionar y recuperar datos de cualquier carga de trabajo y desde cualquier ubicación, todo desde un **único panel de control**. Además, elimina la necesidad de pagar más por integrar herramientas adicionales que, en última instancia, crean brechas y vulnerabilidades. Commvault Cloud y su motor con tecnología de IA siempre activo ofrecen una plataforma unificada que protege todas sus cargas de trabajo contra amenazas en evolución, al tiempo que garantiza una recuperación rápida y, lo más importante, limpia.

83%

de las organizaciones consideran que sería deseable consolidar sus sistemas con un solo proveedor.[4]

Un TCO 5 veces menor

El coste total de propiedad de Commvault es cinco veces menor al de otras herramientas de protección nativas de nube.[5]

4 Forta, Digital Guardian Data Protection, "**Top Considerations for CISOs When Consolidating Information Security Solutions**", abril de 2023.
5 Análisis del TCO del cliente de Commvault.

IA avanzada que permite capacidades de última generación

Como directivo responsable de la seguridad de los datos de su organización, usted debe combatir la amenaza con sus mismas armas. Las amenazas actuales con tecnología de IA exigen actuar con rapidez, implementar medidas de seguridad de datos tempranas y prepararse para una recuperación a gran escala.

"La velocidad de detección es un elemento clave para mitigar el impacto de las intrusiones, y la detección, en particular, requiere que una automatización efectiva. Sin embargo, la mayoría de las organizaciones todavía están en el camino hacia la detección y la generación de informes totalmente automatizados".[2]
IDC: *The Cyber-resilient Organization: Maximum Preparedness with Bullet-proof Recovery*

Commvault Cloud, con tecnología Metallic AI, utiliza inteligencia artificial, aprendizaje automático (ML) y automatización para ofrecer la inteligencia de protección de datos más avanzada de la industria. Capaz de predecir las amenazas con mayor antelación, garantiza recuperaciones más limpias y acelera los tiempos de respuesta.

Servicios de plataforma innovadores

La plataforma Commvault Cloud permite a los equipos de TI y de seguridad gestionar procesos de forma más eficiente y rentable.

Hemos revolucionado la seguridad de los datos y la ciberrecuperación mediante una defensa en capas aplicada a través de una experiencia simple y unificada similar a SaaS. Nuestras capacidades probadas se ofrecen a través de una gama de servicios de plataforma que lo abarca todo: desde alertas tempranas hasta recuperación rápida de todos los datos, para cualquier carga de trabajo y en cualquier lugar.

El 92%

de las organizaciones planean utilizar la IA y el aprendizaje automático para reforzar su ciberseguridad.[6]

Alerta temprana	Gobernanza del riesgo
Detecte antes las amenazas, minimice el radio de afectación y reduzca su exposición al riesgo.	Mejore la postura de seguridad de sus datos localizando y remediando proactivamente los riesgos en sus datos de producción y copia de seguridad.
Preparación y respuesta	**Ciberrecuperación**
Garantice la resiliencia con preparación avanzada, validación automatizada y pruebas de recuperación continuas.	Garantice una recuperación rápida, con la flexibilidad de reponerse de cualquier lugar a cualquier lugar a gran escala.

6 Synchro Works Consulting, "**The Value of Danger of AI in Cybersecurity**", agosto de 2023.

Commvault ofrece una gama gama de capacidades de detección, seguridad y recuperación para reducir el riesgo, minimizar el impacto de los ataques y ofrecer una continuidad empresarial inquebrantable frente a las amenazas. Proteja rápida y fácilmente su entorno de datos con estas funciones:

- **"Air Gapping" e inmutabilidad**: protege los datos de backup en un sitio de almacenamiento seguro y aislado con estrictos controles de acceso para evitar manipulaciones.
- **Validación de punto de restauración limpio**: la automatización con tecnología de IA verifica y garantiza puntos de recuperación limpios, previene la reinfección y proporciona conjuntos de datos impecables.
- **Gestión de la postura de seguridad de los datos**: identifique, analice y proteja archivos confidenciales para reducir los riesgos de filtración en todos sus conjuntos de datos de producción y copia de seguridad.
- **Alerta temprana**: detecte amenazas antes del cifrado, la exfiltración o el daño con tecnología patentada de alerta temprana que descubre y desvía las amenazas avanzadas y de día cero antes de que lleguen a sus datos. Sus activos y entornos de copia de seguridad se ocultan a los atacantes.
- **Resiliencia y recuperación**: elimine los riesgos de malware, evite la reinfección y organice restauraciones a gran escala con una recuperación rápida y fiable.
- **Información de seguridad**: Obtenga visibilidad de extremo a extremo y gestione con eficiencia los riesgos de datos. Reaccione antes y limite la exposición a través de un único panel.
- **Arquitectura de confianza cero**: vaya más lejos con la autenticación multifactor y multipersona; gestión de acceso privilegiado (PAM); herramientas de gestión de identidad y acceso (IAM) como CyberArk, YubiKey; y sistemas biométricos como AAL3.

COMMVAULT CLOUD UNE TI Y OPERACIONES DE SEGURIDAD:

Al implementar Commvault Cloud, su organización se beneficiará de una total seguridad y capacidad de recuperación de sus datos en la nube híbrida, lo que le permitirá visualizar, gestionar y recuperar sus datos dondequiera que se encuentren.

Commvault ofrece a sus clientes una clara ventaja a la hora de garantizar su resiliencia en caso de ciberataque. Para hacerlo hemos dedicado años a innovar y ser líderes en el sector, con más de 1.500 patentes. Una de las ventajas más poderosas que ofrece Commvault Cloud es una arquitectura única creada para el mundo híbrido que ofrece la recuperación masiva más predecible, rápida y rentable del mercado.

Libere el poder de la ciberresiliencia integral

Para obtener más información, visite **www.commvault.com** o **solicite una demostración**.