backupify
A Kaseya COMPANY

5 PRINCIPALES

Puntos ciegos de las copias de seguridad

en Google Workspace

Los 5 principales puntos ciegos de las copias de seguridad en Google Workspace

En los últimos años, los entornos comerciales han experimentado cambios drásticos, transformando no solo la forma en que trabajamos, sino también el lugar desde donde trabajamos. Las empresas modernas dependen cada vez más de las aplicaciones de software como servicio (Software-as-a-Service, SaaS) para hacer frente a estos cambios. Hoy en día, las aplicaciones SaaS se han convertido en herramientas indispensables para las empresas de todo el mundo. Estas soluciones basadas en la nube ofrecen escalabilidad, flexibilidad y rentabilidad, lo que permite a las empresas optimizar las operaciones, mejorar la colaboración y aumentar la productividad. Entre las innumerables ofertas de SaaS, Google Workspace (anteriormente G Suite) se destaca como líder en el ecosistema empresarial.

Desde la administración profesional del correo electrónico hasta el almacenamiento en la nube y el intercambio de archivos, Google Workspace abarca un conjunto de herramientas poderosas diseñadas para admitir diversas funciones comerciales. Estas herramientas se integran sin problemas, proporcionando una plataforma cohesiva que promueve la colaboración y la comunicación dentro de las organizaciones. Aunque Google Workspace ofrece múltiples beneficios a empresas de todos los tamaños, la pregunta sigue siendo: ¿Confiar únicamente en la protección nativa del proveedor de servicios en la nube es suficiente para proteger sus datos?

En este documento técnico, analizamos más detenidamente las posibles brechas de seguridad en la protección nativa de Google. También hemos identificado riesgos clave y puntos ciegos dentro de Google Workspace para ayudarle a proteger mejor sus datos y cargas de trabajo. Siga leyendo para obtener más información sobre estos riesgos y cómo reforzar su estrategia de protección de datos de Google Workspace.

Comprensión de la protección nativa de Google

Si bien Google ofrece características de protección de datos nativas para ayudarle a proteger sus datos, existen brechas notables en su protección nativa que debe abordar para proteger los datos de su organización de manera efectiva.

Opciones nativas de copia de seguridad y recuperación

Google Vault es una poderosa herramienta de archivo diseñada para la retención de datos a largo plazo y el cumplimiento legal. Ayuda a las organizaciones a preservar de manera segura los datos corporativos, garantizando que cumplan con las necesidades regulatorias y de eDiscovery. Con Google Vault, puede buscar, retener, conservar y exportar datos de Google Workspace con facilidad.

Esto hace que la gestión de auditorías, retenciones legales y consultas regulatorias sea simple y eficiente. Sin embargo, es posible que Google Vault no sea la mejor solución de copia de seguridad para los datos de su organización, ya que el proceso de restauración es tedioso y lleva mucho tiempo. Google Vault no admite la restauración directa de archivos a Google Drive o Gmail.

Google replica copias en tiempo real y casi en tiempo real de los datos de producción para garantizar la disponibilidad y respaldar la recuperación ante desastres. Sin embargo, no mantiene copias de seguridad de los datos de Google Workspace específicamente para fines de restauración. Para lograr una continuidad efectiva del negocio, necesita instantáneas diarias y puntuales de sus datos. Lamentablemente, ninguna edición de Google Workspace ofrece estas copias de seguridad.

Puede recuperar los archivos eliminados en Google Drive. Sin embargo, depender de las carpetas de elementos eliminados para la recuperación de datos no es práctico para la mayoría de las organizaciones. Este método es lento, manual, complicado y propenso a fallar. Desafortunadamente, Google Workspace carece de opciones de restauración de datos granulares en todas las ediciones, lo que dificulta la recuperación eficiente de datos específicos.

Redundancia y disponibilidad de datos

Desde servidores hasta servicios de software, cada componente de la plataforma de Google está diseñado para ser altamente redundante, lo que garantiza una baja latencia y una alta disponibilidad. Sus centros de datos distribuidos globalmente evitan que las interrupciones afecten el servicio. En caso de fallas regionales, los datos se transfieren sin problemas entre las instalaciones, lo que permite a los usuarios de Google Workspace trabajar sin interrupciones. Para proteger contra la pérdida de datos y el tiempo de inactividad, Google emplea la replicación de datos en vivo en múltiples centros, lo que garantiza que cualquier acción en Google Workspace se refleje instantáneamente.

A pesar de esto, la mayoría de los incidentes de seguridad en la nube son el resultado directo de una configuración incorrecta. En un incidente reciente, un error de configuración de Google Cloud eliminó la cuenta en la nube de UniSuper. El incidente afectó a casi 600.000 clientes de UniSuper, que no pudieron acceder a sus cuentas durante una semana.

Recuperación de datos

Las opciones de recuperación integradas de Google solo pueden recuperar datos perdidos dentro de un plazo específico, a menudo solo de 25 a 30 días. Esta limitación representa un riesgo para las empresas que necesitan restaurar datos más allá de este período.

Tomemos el ejemplo de los archivos en la papelera para facilitar la comprensión. Los archivos en la papelera de Drive se pueden eliminar de dos maneras: En primer lugar, de forma predeterminada, y en segundo lugar, un usuario puede eliminar manualmente los elementos de la papelera.

Google Drive elimina archivos de la carpeta papelera 30 días después de que se trasladan allí. Un administrador de Google Workspace puede recuperar archivos eliminados de la papelera durante un máximo de 25 días. No pueden recuperar datos una vez que este período haya finalizado. Según IBM, en promedio, las organizaciones tardaron 207 días en identificar el compromiso de los datos en 2023, mucho después de que el período de retención de 30 días había finalizado gradualmente.

Limitaciones de la protección nativa

La protección nativa de Google dentro de sus servicios en la nube, incluidos Google Workspace y Google Cloud Platform, ofrece características de seguridad básicas diseñadas para proteger los datos de los usuarios. Sin embargo, si bien la protección nativa de Google forma una base sólida, se centra principalmente en la seguridad "de" la infraestructura de la nube en lugar de los datos administrados "en" la nube por los usuarios. Esto significa que, si bien Google protege el hardware y el software subyacentes, los usuarios (usted) deben tomar medidas adicionales para proteger sus datos de eliminaciones accidentales, amenazas internas y ataques cibernéticos avanzados.

El modelo de responsabilidad compartida

A medida que las empresas dependen cada vez más de servicios en la nube como Google Workspace, comprender el modelo de responsabilidad compartida se vuelve crucial para una gestión y seguridad de datos efectivas. Este modelo delinea las obligaciones de seguridad entre el proveedor de servicios en la nube (Cloud Service Provider, CSP) y el cliente, lo que garantiza que ambas partes desempeñen un papel en el mantenimiento de un entorno de nube seguro.

En el modelo de responsabilidad compartida, el CSP es responsable de garantizar la seguridad "de" la nube, incluida la infraestructura física, el hardware y el software. Por otro lado, los clientes (usted) son responsables de la seguridad "en" la nube. Esto implica administrar los controles de acceso, configurar sus aplicaciones de manera segura y proteger sus datos.

El modelo de responsabilidad compartida enfatiza que, si bien los CSP proporcionan una seguridad sólida para su infraestructura, los clientes deben administrar y proteger proactivamente sus datos y aplicaciones. El siguiente diagrama muestra cómo se comparten las responsabilidades entre el CSP y el cliente en un modelo de responsabilidad compartida.

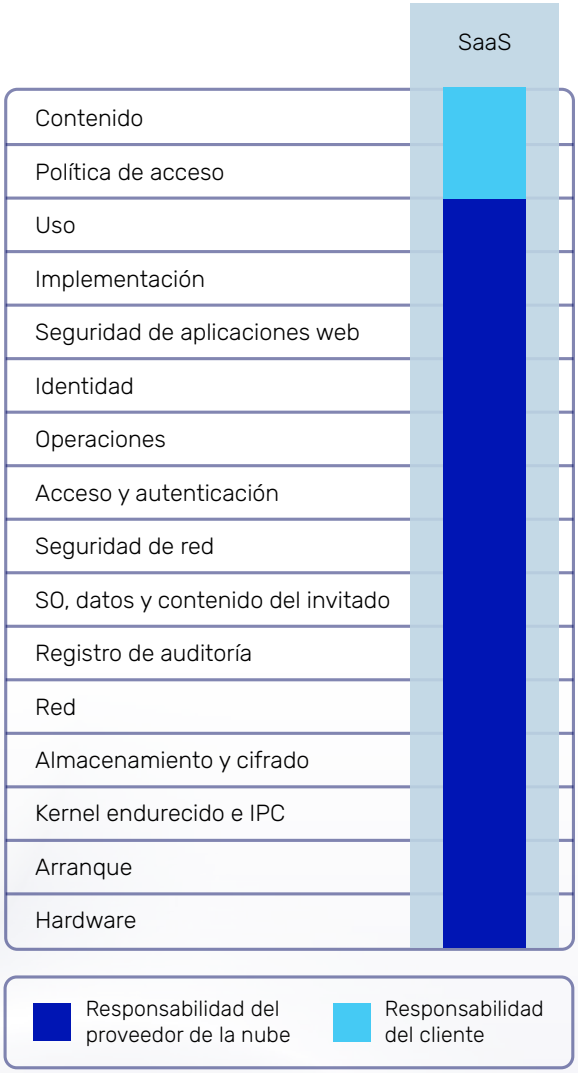


Figura 1: Modelo de responsabilidad compartida

Fuente: Google

Reglas de retención y sus restricciones

Google Workspace ofrece opciones flexibles de retención de datos para ayudar a las organizaciones a gestionar las necesidades regulatorias y de cumplimiento. Por lo general, los datos permanecen en las cuentas de usuario hasta que el usuario o administrador los elimina manualmente. Sin embargo, para las organizaciones que requieren más control sobre sus datos, Google Vault ofrece la capacidad de establecer reglas de retención personalizadas. Estas reglas permiten a los administradores determinar cuánto tiempo deben almacenarse los datos y cuándo deben eliminarse automáticamente. Al establecer estos parámetros, las empresas pueden garantizar que los datos se conserven de acuerdo con sus políticas y requisitos normativos, al mismo tiempo que purgan de manera eficiente los datos que ya no son necesarios. Sin embargo, debe tener mucho cuidado al crear o modificar reglas de retención, ya que una configuración incorrecta puede provocar la eliminación permanente de datos.

ADVERTENCIA: Una regla de retención configurada incorrectamente podría permitir que los servicios de Google purguen datos de inmediato e irreversiblemente. Tenga cuidado al crear o cambiar reglas de retención. Le recomendamos que pruebe nuevas reglas en un pequeño grupo de usuarios antes de aplicarlas a toda su organización.

Figura 2: Advertencia de servicios de Google para crear o modificar reglas de retención

Tipos de pérdida de datos no cubiertos

Google Workspace ofrece varias características de seguridad nativas, como cifrado de datos, autenticación de dos factores y mecanismos antiphishing. Sin embargo, estas medidas no son infalibles.

Además, la seguridad de Google Workspace no cubre de manera integral amenazas internas maliciosas, eliminaciones accidentales o ataques de ransomware, lo que deja los datos confidenciales de su organización vulnerables a la pérdida o corrupción.

Riesgos clave y cinco puntos ciegos principales en Google Workspace

Muchas empresas hoy en día confían sus datos a los proveedores de servicios en la nube, creyendo que las protecciones nativas son suficientes para proteger su valiosa información. Sin embargo, confiar únicamente en estas medidas de seguridad incorporadas puede ser riesgoso.

Si bien los proveedores de la nube, como Google Workspace, ofrecen características de seguridad esenciales, no cubren todas las vulnerabilidades. Estos son los cinco principales puntos ciegos de copia de seguridad en Google Workspace que debe tener en cuenta para proteger sus cargas de trabajo críticas de manera efectiva.

1

ERROR HUMANO

El error humano es uno de los riesgos más frecuentes en Google Workspace. Algunos de los más comunes son:

Eliminaciones y sobreescrituras accidentales

Las eliminaciones y sobreescrituras accidentales pueden ocurrir cuando los empleados eliminan por error archivos críticos o reemplazan datos existentes con versiones incorrectas.

Corrupción involuntaria de datos

La corrupción involuntaria de datos es otra preocupación, donde los archivos pueden volverse inutilizables debido a cambios involuntarios o manejo inadecuado. Estos errores pueden interrumpir los flujos de trabajo y provocar una pérdida de datos significativa si no se abordan de inmediato. De acuerdo con el Informe de Investigaciones de Violación de Datos de Verizon de 2024, el 68% de las violaciones se vincularon a factores humanos no intencionales, como personas que son presas de ataques de ingeniería social o cometen errores.

2

ACTIVIDADES MALICIOSAS

Google Workspace no es inmune a actividades maliciosas.

Amenazas internas

Las amenazas internas representan un riesgo sustancial, en el que los empleados descontentos o aquellos con motivos ulteriores podrían eliminar deliberadamente o filtrar información confidencial. El informe de Verizon también descubrió que los actores internos eran responsables del 35 % de las violaciones.

Ataques cibernéticos externos

Los ciberataques externos, incluidos el phishing y el malware, también pueden comprometer la seguridad de los datos. A menudo, los atacantes apuntan a las cuentas de Google Workspace para obtener acceso no autorizado a información comercial confidencial, lo que podría provocar filtraciones de datos y pérdidas financieras. El informe global de amenazas de 2024 de CrowdStrike reveló un enorme aumento del 75% en las intrusiones en el entorno de la nube en 2023 en comparación con 2022.

3 RIESGOS LEGALES Y DE CUMPLIMIENTO

Los riesgos legales y de cumplimiento son fundamentales para las organizaciones que manejan información confidencial.

Limitaciones de la política de retención y requisitos reglamentarios

Es posible que las políticas de retención nativas de Google Workspace no cumplan con todos los requisitos normativos, especialmente para industrias con estrictas reglas de conservación de datos. Las empresas deben asegurarse de que puedan mantener los datos durante los períodos requeridos para cumplir con las regulaciones y evitar sanciones.

Retenciones legales y desafíos de eDiscovery

Las retenciones legales y los desafíos de eDiscovery surgen cuando las organizaciones necesitan preservar datos para litigios o investigaciones. Estos a menudo requieren herramientas avanzadas más allá de las capacidades nativas de Google para administrar y recuperar la información requerida de manera eficiente.

4 INTEGRACIONES DE APLICACIONES DE TERCEROS

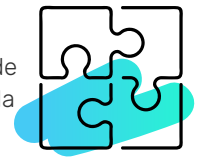
La integración de aplicaciones de terceros con Google Workspace mejora la funcionalidad, pero introduce riesgos adicionales.

Riesgos asociados con aplicaciones de terceros conectadas

Las aplicaciones de terceros pueden agregar conveniencia y aumentar la eficiencia. Sin embargo, se debe tener precaución al integrar aplicaciones y extensiones de terceros. Muchas aplicaciones de terceros pueden ser útiles, pero no necesariamente confiables. Cuando otorga permiso a dichas aplicaciones para acceder y administrar los datos de su organización, pueden cifrar archivos o robar o exponer información confidencial.

Pérdida de datos a través de conexiones API

Las interfaces de programación de aplicaciones (Application Programming Interfaces, API) que conectan aplicaciones pueden exponer inadvertidamente los datos a vulnerabilidades, lo que conduce a un acceso no autorizado o a la pérdida de datos. Garantizar que las integraciones de terceros cumplan con las mejores prácticas de seguridad es crucial para mantener la integridad de los datos.



5 INTERRUPCIONES DEL SERVICIO Y TIEMPO DE INACTIVIDAD

A pesar de la infraestructura confiable de Google, las interrupciones del servicio y el tiempo de inactividad aún pueden ocurrir.

Interrupciones en el servicio de Google

En mayo de 2024, Google sufrió una interrupción masiva que afectó a miles de usuarios en todo el mundo. Dichas interrupciones pueden detener las operaciones comerciales, afectando la productividad y la comunicación. Su empresa debe tener planes de contingencia para gestionar y mitigar el impacto de las interrupciones inesperadas del servicio, lo que garantiza la continuidad durante las operaciones críticas.

Inquietudes sobre la continuidad del negocio

Google Workspace proporciona una base sólida para la productividad y la colaboración, pero no está libre de riesgos. Los errores humanos, las fallas de software, las amenazas internas, las estafas de phishing y los ataques de ransomware representan una amenaza constante para su entorno de Google Workspace, lo que podría provocar la posible pérdida de datos o interrumpir las operaciones comerciales. Según el informe Cost of a Data Breach de IBM de 2023, más del 80% de las violaciones involucraron datos almacenados en entornos de nube.

Mitigación de puntos ciegos de las copias de seguridad

Para proteger sus datos en Google Workspace de manera efectiva, debe adoptar estrategias integrales que vayan más allá de confiar en las funciones de seguridad nativas de Google.

Estrategias integrales de copia de seguridad

La implementación de soluciones confiables de copias de seguridad de terceros es crucial, ya que proporcionan opciones de recuperación de datos extendidas y protegen contra eliminaciones accidentales, errores programáticos y actividades maliciosas. Las soluciones de copia de seguridad de proveedores reconocidos como Datto SaaS Protection también ofrecen funciones avanzadas como opciones de recuperación granular y copias de seguridad automatizadas, lo que garantiza la integridad y disponibilidad de los datos.

Mejores prácticas de protección de datos

Las auditorías periódicas y la capacitación especializada de los empleados son vitales para fortalecer la seguridad general y la resiliencia de su entorno de Google Workspace. Realizar auditorías de seguridad frecuentes ayuda a identificar y abordar las vulnerabilidades, garantizando el cumplimiento de las mejores prácticas y los requisitos normativos. Las auditorías deben cubrir controles de acceso, integraciones de terceros y políticas de gestión de datos.

Igualmente importante es construir una cultura de concientización sobre la seguridad a través de programas continuos de capacitación para empleados. Educar al personal sobre cómo reconocer los intentos de phishing, el manejo seguro de datos y la comprensión de la importancia de las medidas de seguridad les permite actuar como la primera línea de defensa contra posibles amenazas.

Política y gobernanza

Crear políticas sólidas de gobernanza de datos es esencial para proteger los datos en Google Workspace y cumplir con los estándares regulatorios. Esto incluye establecer pautas claras sobre la clasificación de datos, los controles de acceso y las políticas de retención. La gobernanza efectiva de los datos le ayuda a mantener la integridad de los datos, mitigar los riesgos asociados con las filtraciones de datos y cumplir con las regulaciones de la industria.

También es importante que alinee sus estrategias de copia de seguridad con estas políticas de gobernanza y requisitos de cumplimiento. Las opciones de copia de seguridad nativas de Google Workspace a menudo no cumplen con los estrictos estándares regulatorios, como el GDPR o la HIPAA, que exigen períodos de retención de datos específicos y la capacidad de restaurar datos de puntos particulares en el tiempo. La implementación de soluciones integrales de copias de seguridad de terceros garantiza que su organización pueda cumplir con estos requisitos al permitirle retener datos durante períodos más prolongados y proporcionar un medio confiable para recuperar datos durante auditorías o investigaciones legales.

"Las soluciones de copia de seguridad de proveedores reconocidos como Datto SaaS Protection también ofrecen funciones avanzadas como opciones de recuperación granular y copias de seguridad automatizadas, lo que garantiza la integridad y disponibilidad de los datos".

Evaluación de soluciones de copia de seguridad de terceros

Las soluciones de copia de seguridad de terceros proporcionan políticas de retención más extendidas, lo que permite la recuperación de datos más antiguos y la protección contra la pérdida prolongada de datos. También actúan como una red de seguridad, llenando las brechas que dejan las protecciones nativas y brindando la tranquilidad de que los datos comerciales críticos son seguros y recuperables en cualquier escenario. Estos son algunos criterios para considerar al evaluar soluciones de copia de seguridad de terceros para Google Workspace.

Compatibilidad con Google Workspace

Un factor crítico al seleccionar una solución de copia de seguridad es garantizar que se integre sin problemas con Google Workspace. La solución debe admitir todas las aplicaciones principales, incluidos Gmail, Google Drive, unidades compartidas, calendarios y contactos. Esta compatibilidad garantiza que todos los datos dentro del entorno se respalden adecuadamente y se puedan restaurar cuando sea necesario.

Características de seguridad

La seguridad es primordial en la copia de seguridad de datos. Busque soluciones que ofrezcan métodos de cifrado sólidos tanto en tránsito como en reposo y protejan los datos del acceso no autorizado. Su solución de copia de seguridad debe incluir controles de acceso, lo que permite a los administradores definir quién puede acceder y administrar las copias de seguridad. Las opciones de recuperación granular también son esenciales, lo que permite la restauración de archivos o correos electrónicos específicos sin tener que realizar una recuperación completa.

Otra característica importante son las copias de seguridad automatizadas, que garantizan una protección de datos uniforme sin necesidad de intervención manual.

Facilidad de uso e implementación

Considere una solución de copia de seguridad fácil de implementar y de usar. Esto es esencial para mantener la productividad y evitar el tiempo de inactividad durante la fase de configuración. Una interfaz intuitiva reduce la curva de aprendizaje, lo que permite a sus equipos aprovechar todas las capacidades de la solución de copia de seguridad sin extensos períodos de incorporación o capacitación.

Reputación y apoyo del proveedor

Es importante considerar la reputación del proveedor de soluciones de copia de seguridad antes de cerrar el acuerdo. Asegúrese de buscar proveedores con un sólido historial de protección de datos y que reciban reseñas positivas de clientes satisfechos. Cuando se trata de protección y recuperación de datos, cada segundo importa. Por lo tanto, la asistencia confiable al cliente es fundamental. Su proveedor de copias de seguridad debe ofrecer asistencia con los procesos de configuración, resolución de problemas y recuperación.

Otro factor crítico es la flexibilidad y la escalabilidad. A medida que su negocio se expanda, sus requisitos de protección de datos también cambiarán. Busque un proveedor de copias de seguridad que ofrezca flexibilidad y escalabilidad, lo que permite que el sistema de copias de seguridad se expanda sin problemas a medida que aumentan los requisitos de datos de su organización. Esta adaptabilidad garantiza que su solución de copia de seguridad siga siendo eficaz y relevante con el tiempo.

Disfrute de la protección de datos de Google Workspace sin esfuerzo con Datto SaaS Protection

Dadas las posibles brechas de seguridad en Google Workspace, la implementación de una solución de copia de seguridad de terceros de vanguardia es una ventaja para las empresas que buscan fortalecer la seguridad general y la resiliencia de sus cargas de trabajo de misión crítica.

Datto SaaS Protection es una solución de copia de seguridad "de única configuración" para Google Workspace que le ahorra tiempo, esfuerzo y dinero. Además de las opciones de recuperación granular y restauración en un momento determinado, nuestra solución también proporciona copias de seguridad automatizadas tres veces al día, lo que garantiza que sus datos críticos en todas sus aplicaciones clave estén actualizados y tengan una copia de seguridad constante. También tiene la opción de solicitar copias de seguridad a pedido en cualquier momento.

Datto SaaS Protection es increíblemente fácil de usar. En solo cinco minutos, puede configurar y comenzar a proteger sus datos de Google Workspace.

Datto SaaS Protection hace que recuperar datos perdidos sea rápido y fácil, no semanas o días, con solo unos pocos clics.

Además, nuestro enfoque multicapa de seguridad protege sus datos del ransomware y otras amenazas.

¿Está listo para tomar el control total de sus datos? **Vea la demostración interactiva** para descubrir cómo Datto SaaS Protection puede transformar la forma en que administra y protege sus datos de Google Workspace.

HAGA UN RECORRIDO DE PRODUCTOS

backupify
A Kaseya COMPANY

Sede corporativa
Kaseya Miami
701 Brickell Avenue
Suite 400
Miami, FL 33131
partners@datto.com
www.datto.com
888.294.6312

Oficinas globales
USA: 888.294.6312
Canada: 877.811.0577
EMEA: +44 (0) 118 402 9606
Australia: +61 (02) 9696 8190
Singapore: +65-31586291

Julio de 2024