Gartner

Licensed for Distribution

Magic Quadrant para soluciones de software de copia de seguridad y recuperación empresarial

Publicado el 7 de agosto de 2023 - ID G00776884 - 43 minutos de lectura

Por los analistas: Michael Hoeck, Nik Simpson, Jerry Rozeman, Jason Donham

A medida que las empresas amplían su uso de entornos híbridos y multinube y aplicaciones SaaS, mientras gestionan la amenaza adaptativa de los ataques de ransomware, los líderes de I&O deben evaluar continuamente sus capacidades de copia de seguridad y recuperación. Esta investigación proporciona análisis de proveedores de copias de seguridad y recuperación.

Definición o descripción del mercado

Gartner define las soluciones de software de copia de seguridad y recuperación empresarial como soluciones desarrolladas por proveedores que capturan una copia en el momento (copia de seguridad) de las cargas de trabajo empresariales en entornos locales, híbridos, multinube y SaaS. Estas soluciones escriben los datos en un destino de almacenamiento secundario con el fin de recuperar estos datos en caso de pérdida. Pueden ofrecerse como dispositivos de solo software, hardware o virtualizados, o como copias de seguridad como servicio (BaaS) basadas en SaaS.

Proteger y recuperar los datos de las aplicaciones empresariales independientemente del tipo de infraestructura subyacente y de la ubicación es ahora más crítico que nunca. A medida que las empresas avanzan hacia entornos más complejos que incluyen cantidades masivas de datos, se espera que las soluciones de software de copia de seguridad y recuperación empresariales protejan estas cargas de trabajo, ya sea que residan en entornos locales, híbridos, multinube o SaaS.

Las soluciones de software de copia de seguridad y recuperación empresariales son vitales para la capacidad de una organización de recuperar datos después de eventos que hacen que los datos sean inaccesibles. Ya sea que el evento sea accidental, malicioso o ambiental, las organizaciones utilizan estas soluciones para recuperar y restaurar eficazmente el acceso a los datos afectados.

Las soluciones deben ofrecer capacidades eficaces para simplificar la gestión de la protección de datos en entornos empresariales complejos. También deben garantizar una recuperación fiable al proteger los datos de las copias de seguridad contra un panorama de amenazas en constante

cambio, y acelerar y organizar las respuestas de recuperación de datos ante desastres tradicionales y eventos de ransomware.

Las capacidades imprescindibles de una solución de copia de seguridad y recuperación incluyen:

- Copia de seguridad y recuperación de datos ubicados en la infraestructura del centro de datos en entornos locales, incluidos sistemas operativos, archivos, bases de datos, máquinas virtuales y aplicaciones.
- Copia de seguridad y recuperación de datos ubicados en infraestructura de nube pública, incluidas nubes híbridas y multinube, arquitecturas y entornos como infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y SaaS.
- Crear varias copias puntuales de la copia de seguridad para respaldar la resistencia, la recuperación ante desastres y otros casos de uso.
- Asignación de múltiples políticas de copia de seguridad y retención que se alineen con los objetivos de recuperación puntual y temporal de la organización.
- Informar el éxito y el fracaso de las tareas de copia de seguridad/recuperación.

Las capacidades estándar de una solución de copia de seguridad y recuperación incluyen:

- Organizar por niveles los datos de la copia de seguridad en múltiples destinos, incluidos la nube pública, el proveedor de la copia de seguridad y recuperación y el almacenamiento de objetos.
- Integración con destinos de almacenamiento de copias de seguridad inmutables o con el propio almacenamiento inmutable del proveedor de copias de seguridad y recuperación.
- Organizar pruebas y procesos de recuperación ante desastres y ransomware.
- Consola centralizada para la gestión de la infraestructura de soluciones de copia de seguridad distribuida.

Las capacidades opcionales que puede proporcionar la solución incluyen:

- Ampliar los casos de uso de datos de copia de seguridad para respaldar el descubrimiento de datos, el cumplimiento, la gestión de copias de datos, la prueba/desarrollo y el descubrimiento electrónico.
- Proteger otras cargas de trabajo, incluidos contenedores, almacenamiento de objetos, sitios y terminales de sucursales remotas/periféricas.

- Detección de malware y anomalías de datos de ransomware desarrolladas o integradas por el proveedor.
- Bóvedas de datos inmutables o entornos de recuperación aislados.
- Recuperación sin servidor

Magic Quadrant

Figura 1: Magic Quadrant para soluciones de software de copia de seguridad y recuperación empresarial

Puntos fuertes y precauciones del proveedor

Acronis

Acronis es un Especialista en este Magic Quadrant. La cartera de copias de seguridad de Acronis consta de su solución en entornos locales Acronis Cyber Protect y la oferta alojada en la nube Acronis Cyber Protect Cloud. Ambas proporcionan copia de seguridad integrada y gestión de terminales para servidores físicos, máquinas virtuales (virtual machines, VM) en entornos locales, cargas de trabajo SaaS, cargas de trabajo de IaaS en la nube pública y terminales. La mayoría de sus clientes están en el mercado intermedio. Un equipo de ventas directas y más de 20 000 proveedores de servicios entregan los productos a través de 52 centros de datos de Acronis repartidos en las principales zonas geográficas. Durante el periodo de evaluación, Acronis añadió varias funciones nuevas. Estas incluyen soporte para la función de bloqueo de retención DD de Dell PowerProtect, recuperación con un clic, recuperación iniciada por el usuario final desde la última copia de seguridad conocida, validación de copia de seguridad asistida por aprendizaje automático (machine learning, ML) y recuperación ante desastres y recuperación ante fallos para máquinas virtuales de Microsoft Azure a la nube de Acronis.

Puntos fuertes

- Capacidades integradas de protección cibernética y de datos para terminales, servidores de aplicaciones e implementaciones de IaaS en la nube pública: Acronis ofrece una oferta única basada en agentes que combina seguridad, copia de seguridad y recuperación ante desastres (disaster recovery, DR) y administración de TI para terminales, estaciones de trabajo, servidores de aplicaciones e implementaciones de IaaS en la nube pública en Azure y AWS.

- Amplio soporte para hipervisores: Acronis ofrece soporte para un amplio conjunto de hipervisores más allá de VMware y Microsoft, como Citrix XenServer, Virtuozzo, Red Hat, Oracle VM, Nutanix, Linux KVM y Scale Computing.

- Cobertura global en varios idiomas: Acronis ofrece una solución de protección de datos diferenciada y disponible a nivel mundial para sitios remotos/ubicaciones periféricas para servidores y terminales localizados en más de 25 idiomas.

Precauciones

- Capacidades limitadas de la nube pública y empresarial: Acronis carece de capacidades empresariales críticas, con soporte limitado para bases de datos empresariales, arquitecturas de clúster, sistemas operativos, almacenamiento conectado a la red (network-attached storage, NAS), integración de almacenamiento empresarial, agrupación de almacenamiento, deduplicación y soporte de aplicaciones en la nube pública.

- Escalabilidad limitada: La arquitectura de almacenamiento directo a copia de seguridad configurada por el agente de Acronis es menos adecuada para implementaciones de grandes empresas debido a la falta de funcionalidades empresariales y la escalabilidad limitada.

- Enfoque comercial en proveedores de servicios gestionados (managed service providers, MSP): Acronis se centra principalmente en la venta a través de MSP para proporcionar una solución gestionada que brinde copias de seguridad, DR, ciberseguridad, colaboración y gestión de terminales. Con este enfoque de salida al mercado, las relaciones comerciales y la experiencia del cliente, incluidos el soporte, la seguridad y el rendimiento, serán una responsabilidad principal del MSP elegido.

Arcserve

Arcserve es un Contendiente en este Magic Quadrant. La cartera de copias de seguridad de Arcserve incluye Arcserve UDP, Arcserve Backup, dispositivos Arcserve UDP, Arcserve Cloud Direct, Arcserve UDP Cloud Hybrid Secured by Sophos, dispositivos de almacenamiento Arcserve OneXafe y Arcserve SaaS Backup. Las operaciones de Arcserve están geográficamente diversificadas y la mayoría de sus clientes se encuentran en el segmento del mercado intermedio. Durante el periodo de evaluación, Arcserve lanzó UDP 9.0, que incluía mejoras para el soporte de bases de datos, una consola de gestión multiusuario alojada en la nube y basada en SaaS, y la capacidad de escribir copias de seguridad directamente en el almacenamiento de objetos compatible con S3. Además de las mejoras de UDP, Arcserve también realizó cambios en dispositivos de copia de seguridad y dispositivos de almacenamiento para mejorar el rendimiento y la escalabilidad.

Puntos fuertes

- Amplio soporte para cargas de trabajo: La combinación de Arcserve Backup y Arcserve UDP proporciona a Arcserve la capacidad de ofrecer soporte a muchas cargas de trabajo empresariales en los centros de datos y la nube pública. Este amplio soporte para cargas de trabajo en combinación con una plataforma escalable y múltiples opciones de integración de destinos de almacenamiento es capaz de proteger múltiples petabytes de datos.

- Almacenamiento de objetos directo a la nube: UDP permite a los clientes realizar copias de seguridad de los datos directamente en el almacenamiento de objetos en la nube con deduplicación. Es compatible con AWS S3, Wasabi y Google Cloud Storage.

- Mejoras de rendimiento y capacidad para dispositivos de almacenamiento OneXafe: Las mejoras de OneXafe proporcionan recuperaciones más rápidas y una mayor escala con un tamaño más pequeño, con almacenamiento en unidad de estado sólido (SSD) disponible y una capacidad de unidad de disco individual superior a 24 TB.

Precauciones

- Capacidades de detección y recuperación limitadas: Arcserve UDP combinado con antimalware Sophos carece de capacidades de detección de anomalías y orientación a los puntos de recuperación recomendados.

- Inmutabilidad limitada de OneXafe: El diseño inmutable de los dispositivos de almacenamiento OneXafe carece de bloqueo de almacenamiento de objetos y controles de autenticación

multipersona, lo que limita sus capacidades óptimas de protección contra la pérdida de datos contra ransomware y amenazas internas.
- Carece de copia de seguridad del contenedor: Arcserve no proporciona capacidades de copia de seguridad para cargas de trabajo de contenedores.

Cohesity

Cohesity es Líder en este Magic Quadrant. Su cartera de productos de copia de seguridad consta de DataProtect y una oferta de BaaS llamada DataProtect entregada como servicio. Las operaciones de Cohesity abarcan Norteamérica, Europa Occidental y Asia/Pacífico. Sus clientes tienden a estar en el mercado intermedio superior y en los segmentos empresariales. Durante el período de evaluación, Cohesity introdujo un almacenamiento en bóveda en la nube administrado por el proveedor llamado FortKnox, que se puede combinar con capacidades de detección de amenazas y clasificación de datos en una nueva solución llamada DataHawk. Agregó integraciones de bases de datos DataProtect para ampliar la cobertura de SAP y admitir PostgreSQL y Couchbase. Además, anunció una asociación OEM con IBM para incluir la protección de datos de Cohesity como parte de la nueva solución Storage Defender de IBM.

Puntos fuertes

- Gestión unificada y simplificada: Cohesity Helios, un plano de control basado en SaaS, proporciona una experiencia administrativa centralizada que es común e intuitiva para todos los productos en su oferta de copias de seguridad.

- BaaS multinube y almacenamiento: Cohesity DataProtect entregado como servicio y los productos FortKnox permiten a los clientes elegir entre múltiples ubicaciones de almacenamiento de plano de datos en la nube, incluidos AWS y Azure.

- Estrategia de alianza de seguridad: Cohesity ha involucrado proactivamente a múltiples proveedores con diversas disciplinas en el mercado de la seguridad. El objetivo de su alianza de seguridad de datos es impulsar soluciones colaborativas y desarrollar productos integrados para abordar de forma más amplia las preocupaciones de los clientes sobre la seguridad de los datos y la resistencia.

Precauciones

- Las nuevas inversiones introducen la dependencia en la tecnología de terceros: La solución DataHawk de Cohesity incluye dependencias en dos nuevas asociaciones OEM para reforzar sus inversiones en ofertas de complementos recientes.

- Capacidades limitadas de BaaS en comparación con las gestionadas por el cliente: Los productos Cohesity y las características relacionadas de FortKnox y DataHawk aún no están disponibles para los clientes que protegen sus datos con su oferta de BaaS, DataProtect entregada como servicio.

- Menos cobertura geográfica: Cohesity se queda atrás con respecto a otros proveedores líderes en presencia y ejecución de mercado en Sudamérica.

Commvault

Commvault es Líder en este Magic Quadrant. Su cartera incluye Commvault Backup & Recovery, Commvault Disaster Recovery, Commvault HyperScale X, la cartera Metallic SaaS y Metallic ThreatWise. Las operaciones de Commvault están geográficamente diversificadas, y sus clientes tienden a ser empresas grandes. Durante el periodo de evaluación, Commvault introdujo soporte para MongoDB Atlas, Hyper-V Live Recovery, Couchbase y Amazon VPC Protection, y una capacidad que escanea el contenido de copia de seguridad en busca de malware durante la recuperación. Commvault mejoró su oferta de Metallic al agregar soporte para bases de datos de Azure, incluidos SQL Server, Cosmos DB, MariaDB, MySQL y PostgreSQL, así como soporte para restauraciones de autoservicio para Exchange Online y OneDrive.

Puntos fuertes

- Alcance de la cobertura de BaaS: La amplia cobertura de aplicaciones SaaS, multinube, en entornos locales y terminales de Commvault Metallic se complementa con la adición de protección de Oracle Cloud Infrastructure (OCI), la incorporación de su propio almacenamiento de objetos OCI y las nuevas ofertas Metallic File and Object Archive y Metallic ThreatWise.

- Interoperabilidad integral basada en software: El software Commvault Backup & Recovery proporciona una amplia cobertura y capacidades para entornos locales, híbridos y multinube. El soporte de nube pública ahora incluye un amplio soporte para Azure, AWS, GCP y OCI.

- Lleva las características empresariales a niveles de precios competitivos: Commvault ha fijado el precio de su licencia por MV para Commvault Backup & Recovery para entrar en nuevos segmentos de mercado que de otro modo no habrían estado disponibles antes.

Precauciones

- Las innovaciones en entornos locales retrasan la cadencia de actualización de la nube: La estrategia de productos de Commvault actualiza Metallic BaaS antes de que estén disponibles características equivalentes para los productos Commvault Complete Data Protection e HyperScale X. Esto da como resultado que las nuevas funciones estén disponibles inicialmente para el subconjunto basado en la nube de la base de clientes de Commvault.

- Experiencia del cliente de Variable Commvault Metallic: Algunos clientes de Gartner han expresado sus preocupaciones por los desafíos asociados con el rendimiento poco uniforme de Metallic y las dificultades de configuración inicial.

- Capacidades de gestión poco uniformes: Las revisiones de Gartner Peer Insights indican que el comando y el control unificados entre la interfaz de usuario HTML5 de Commvault Command Center carecen de algunas características de la consola de aplicaciones local.

Dell Technologies

Dell Technologies es Líder en este Magic Quadrant. Su cartera de software de copia de seguridad y recuperación está compuesta por PowerProtect Data Manager, PowerProtect Cyber Recovery, CyberSense, Dell NetWorker, Dell Avamar, Dell APEX Backup Services, PowerProtect serie DP y dispositivos PowerProtect serie DD. Las operaciones de Dell están geográficamente diversificadas, y sus clientes tienden a ser empresas grandes, con presencia en el mercado intermedio. En los últimos 12 meses, ha mejorado PowerProtect Data Manager para incluir la copia de seguridad y recuperación del Sistema de Archivos Distribuidos de Microsoft, la recuperación a nivel de archivo para Dynamic NAS Protection y la compatibilidad con PowerProtect Cloud Snapshot Manager para Google Cloud. Las nuevas ofertas incluyen PowerProtect Data Manager Appliance (DM5500), PowerProtect Cyber para Azure y Google, y CyberSense para AWS.

Puntos fuertes

- PowerProtect Cyber Recovery para la nube y entornos locales: La solución de recuperación de ransomware y bóveda de datos de Dell, llamada PowerProtect Cyber Recovery, ahora incluye opciones de implementación para entornos locales y en la nube de AWS, Azure y Google.
- Escala de dispositivo PowerProtect DD: La introducción de Smart Scale por parte de Dell permite a los clientes de PowerProtect Data Manager combinar la capacidad de múltiples dispositivos DD de PowerProtect, lo que permite un equilibrio de datos de copia de seguridad simplificado y la migración entre ellos.
- Soporte y disponibilidad multinube de PowerProtect Data Manager: PowerProtect Data Manager proporciona soporte uniforme e integral para cargas de trabajo en AWS, Azure y GCP. También está disponible en los respectivos mercados e incluye licencias para APEX Protection Storage.

Precauciones

- Sin plano de control basado en SaaS: Dell carece de un plano de control integral basado en SaaS e interfaz administrativa común para todos los componentes de su solución, que a menudo se encuentran en las principales soluciones de proveedores.
- Opciones limitadas de almacenamiento de copias de seguridad: Los dispositivos DD de PowerProtect siguen siendo un requisito para el uso de la mayoría de las soluciones de protección de datos de Dell, lo que limita el uso de destinos de copia de seguridad alternativos.
- El análisis avanzado de datos de ransomware requiere un entorno dedicado: La detección avanzada de anomalías y malware requiere un dispositivo DD de PowerProtect independiente y dedicado, así como una infraestructura informática adicional.

Druva

Druva es un Visionario en este Magic Quadrant. La plataforma Druva Data Resiliency Cloud es una oferta de BaaS que aprovecha la infraestructura de AWS para ejecutar, almacenar y administrar copias de seguridad. La plataforma consta de múltiples productos que proporcionan respaldo y recuperación ante desastres (DR) de máquinas virtuales (VM) en entornos locales y en la nube; respaldo y DR nativos de la nube de AWS y de Kubernetes y respaldo de aplicaciones y terminales SaaS. Las operaciones de Druva están geográficamente diversificadas y la mayoría de sus clientes se encuentran en Norteamérica. Sus clientes tienden a estar en el mercado intermedio y en los segmentos empresariales. Durante el periodo de evaluación, Druva añadió Salesforce Data Archiver, Data Lock, Unusual Data Activity y nuevas integraciones como hosts de máquina virtual Windows Server 2022 Hyper-V, SAP HANA, VMware en Azure, VM en Azure Stack y AWS S3. También mejoró la compatibilidad con Nutanix AHV y aceleró la copia de seguridad incremental para NAS con Advanced Smart Scan.

Puntos fuertes

- Alcance de la garantía: Druva Data Resiliency Guarantee ofrece un alcance integral de objetivos de nivel de servicio que incluyen tasa de éxito de copias de seguridad, disponibilidad, inmutabilidad, durabilidad y confidencialidad.

- Arquitectura de soluciones BaaS nativas de la nube: A partir de su solución BaaS madura, Druva ha realizado una inversión significativa en un rediseño no disruptivo para el cliente de su plataforma de arquitectura de copia de seguridad para establecer un nuevo marco para futuras capacidades de escalabilidad, agilidad y multinube.

- Experiencia de centro de datos a cliente en la nube: Muchos clientes transmiten una experiencia positiva en el uso de BaaS de Druva para proteger los datos de aplicaciones SaaS, entornos locales y máquinas virtuales en la nube.

Precauciones

- Capacidades limitadas de protección de la carga de trabajo nativa en la nube: Druva ha tardado en ampliar sus ofertas de protección nativa en la nube en comparación con los principales proveedores. Carece de integración sin agente con Azure VM, Google Compute Engine (GCE) y OCI. Las integraciones de carga de trabajo con Azure SQL, Azure Blob Storage, MongoDB y Cassandra no son compatibles.

- Capacidades multinube limitadas: La solución BaaS de Druva se basa únicamente en la arquitectura de nube de AWS para sus planos de control y datos. Se queda atrás con respecto a los principales proveedores que proporcionan a los clientes la opción de ubicaciones de plano de datos multinube para sus ofertas de BaaS y almacenamiento de proveedores.

- Integración de copia de seguridad de aplicaciones SaaS menos completa: La expansión de Druva de la protección de nuevas aplicaciones SaaS es limitada. Carece de soporte para MS Dynamics, Azure AD, ServiceNow, Azure DevOps y GitHub.

HYCU

HYCU es un Visionario en este Magic Quadrant. HYCU Protégé es una plataforma BaaS híbrida y multinube que abarca Azure, AWS y Google para admitir IaaS, DBaaS, PaaS, SaaS y cargas de trabajo en entornos locales. Las operaciones de HYCU están geográficamente diversificadas y la mayoría de sus clientes se encuentran en Norteamérica. Sus clientes tienden a estar en el mercado intermedio superior. Durante el periodo de evaluación, HYCU introdujo varias capacidades nuevas, como un nivel gratuito para AWS, soporte añadido para Azure Government, copia de seguridad de intercambio de archivos sin impacto y cargas de trabajo periféricas y ROBO. Además, HYCU presentó R-Cloud, una plataforma de desarrollo de código bajo para que los proveedores desarrollen copias de seguridad SaaS en la plataforma HYCU, junto con R-Graph, una herramienta capacidad de observación y mapeo de dependencias para cargas de trabajo SaaS.

Puntos fuertes

- Facilidad de uso: Las consultas de los clientes de Gartner indican un alto nivel de satisfacción por la facilidad de uso, la estabilidad del producto y la gestión de copias de seguridad y recuperación ante desastres para la solución de gestión híbrida HYCU Protégé.

- Compatibilidad multinube e híbrida: HYCU Protégé simplifica la protección de entornos multinube e híbridos al admitir cargas de trabajo de Azure, AWS, Google y centros de datos con una única solución SaaS unificada.

- Copia de seguridad SaaS: R-Cloud tiene el potencial de acelerar el soporte para copias de seguridad SaaS más allá de las aplicaciones SaaS más populares, como Microsoft 365 y Salesforce.

Precauciones

- Limitaciones en entornos locales: La oferta para entornos locales de HYCU se queda atrás con respecto a la de los proveedores líderes en características como la deduplicación global de datos, la protección continua de datos (CDP), la compatibilidad con cargas de trabajo de contenedores y clústeres empresariales como Oracle RAC, y la compatibilidad con cargas de trabajo que no sean x86 como Power/AIX.

- Capacidades limitadas de detección de ransomware: A HYCU le falta la detección avanzada de ransomware basada en el análisis de datos de copia de seguridad, como la detección de cifrado y entropía, y las capacidades de orientación de puntos de recuperación que se encuentran en ofertas competitivas.

- El cliente es responsable del almacenamiento y la seguridad en entornos locales: HYCU no tiene control directo sobre el almacenamiento en entornos locales y la seguridad del almacenamiento, lo que hace que los clientes sean responsables de configurar una solución segura para proteger las copias de seguridad contra los ciberataques.

IBM

IBM es un visionario en este Magic Quadrant. Su cartera principal de copias de seguridad consiste en IBM Storage Protect, IBM Storage Protect Plus, IBM Storage Protect Snapshot, IBM Storage Copy Data Management e IBM Storage Protect for Cloud. Las operaciones de IBM están geográficamente diversificadas, y sus clientes tienden a ser empresas grandes. El año pasado, el proveedor lanzó cuatro actualizaciones para Storage Protect y Storage Protect Plus. Las adiciones de Storage Protect incluyen almacenamiento inmutable en IBM Cloud Object Storage, bloqueo de objetos en Amazon S3 y actualizaciones del centro de operaciones. Las incorporaciones de Storage Protect Plus incluyen compatibilidad con clústeres Red Hat OpenShift para IBM Z, SAP HANA y copias de seguridad incrementales para contenedores. Storage Protect for Cloud introdujo soporte para Azure VM, BLOB, AD y File, Salesforce y Microsoft Dynamics 365.

Puntos fuertes

- Estrategia del producto: IBM anunció un cambio estratégico en sus ofertas de copia de seguridad y recuperación integrándolas con su línea de productos de almacenamiento principal y múltiples productos OEM complementarios. Storage Defender está posicionado para ofrecer una solución de protección cibernética integrada y unificada bajo un plano de control común. IBM se asoció con Cohesity para reemplazar sus capacidades actuales de protección de VM y proporcionar el nuevo plano de control basado en SaaS.

- Copia de seguridad de contenedor OpenShift: IBM siguió realizando importantes inversiones en IBM Storage Protect Plus para la copia de seguridad y recuperación de Red Hat OpenShift Kubernetes e IBM Cloud Paks. Las incorporaciones recientes incluyen la protección de entornos OpenShift de Red Hat conectados a clústeres, recursos dentro del alcance de clústeres y espacios de nombres, e integraciones CSI actualizadas con Ceph, almacenamiento de bloques IBM e Hitachi NAS.

- Protección de Microsoft 365: IBM Storage Protect for Cloud ofrece restauración de autoservicio para el usuario final para Microsoft Exchange Online, SharePoint Online, Teams, OneDrive y Groups.

Precauciones

- Cambio de cartera en curso: La estrategia y ejecución de IBM sobre el cambio de cartera anunciado es un trabajo en curso. Esta nueva cartera afectará a los clientes existentes y potenciales a medida que se lancen nuevos productos de sustitución. Los clientes de IBM necesitarán múltiples productos, basados en un mayor número de tecnologías ISV y OEM, para cumplir con sus requisitos de protección de datos multinube e híbridos.

- Ejecución limitada: IBM ha cambiado a menudo su visión y estrategia de producto para la integración y el posicionamiento de los antiguos productos Spectrum Protect y Spectrum Protect

Plus, y ha demostrado un éxito limitado en la ejecución de estos cambios. Esto incluye esfuerzos anteriores para posicionar Spectrum Protect Plus como su oferta líder en el mercado.
- Capacidades limitadas de recuperación multiplataforma: IBM Storage Protect Plus requiere soluciones de recuperación ante desastres integradas de cliente o ISV API o el uso de soluciones de socios ISV para admitir la recuperación multiplataforma.

Microsoft

Microsoft es un especialista y un nuevo participante en este Magic Quadrant. Su cartera de copias de seguridad y recuperación incluye Azure Backup, Azure Site Recovery (ASR), Microsoft Azure Backup Server (MABS), System Center Data Protection (DPM) y Microsoft Azure Recovery Services (MARS). Las operaciones de Microsoft están geográficamente diversificadas y sus clientes tienden a ser de todos los tamaños. En los últimos 12 meses, Microsoft ha añadido varias mejoras a Azure Backup, como Azure Backup Instant Restore, Cross Zonal Restore of Azure VMs, Azure Vault-Archive, nivelación inteligente, análisis de costos de copia de seguridad, bóvedas inmutables, autenticación multiusuario y cifrado mejorado.

Puntos fuertes
- Oferta optimizada para clientes dedicados de Microsoft: Azure Backup y Azure Site Recovery son ofertas adecuadas para copias de seguridad y recuperación ante desastres que protegen las cargas de trabajo para una amplia gama (pequeñas y grandes empresas) de clientes que utilizan principalmente Microsoft Windows y Azure VM en entornos locales.

- Hoja de ruta completa: Microsoft articula una hoja de ruta muy completa con una integración profunda de las funciones existentes y las nuevas por venir para mejorar su cartera de seguridad de copias de seguridad con varias capacidades en modo de vista previa pública o privada.

- Bajo costo total de propiedad (total cost of ownership, TCO): Azure Backup y Azure Site Recovery ofrecen un TCO bajo en comparación con ofertas de terceros de la competencia.

Precauciones
- Cobertura de carga de trabajo mínima: La matriz de soporte de copias de seguridad de Azure se limita a la protección de Microsoft Windows Servers o Microsoft Windows VMs en entornos locales, Azure VMs, SQL Server en Azure VM, SAP HANA en Azure VM, Azure Files, Azure Postgres, Azure Blobs y Azure Disks. Otros servicios PaaS y SaaS de Microsoft como Azure SQL Server, Azure AD, Azure DevOps, Dynamics 365 y Microsoft 365 no están cubiertos.

- Sin soporte multinube: La copia de seguridad de Azure no ofrece soporte para la protección de AWS, Google u otros servicios en la nube o servicios SaaS, ya que está dedicada a Azure y cargas de trabajo en entornos locales.

- Oferta de productos superpuestos: Las opciones de copia de seguridad y recuperación de Microsoft son una combinación compleja de productos múltiples, interconectados y superpuestos.

OpenText

OpenText es un Especialista en este Magic Quadrant. Finalizó su adquisición de Micro Focus en enero de 2023. Su cartera de productos de copia de seguridad empresarial consta principalmente de dos productos: Data Protector para cargas de trabajo en entornos locales y Data Protector para cargas de trabajo en la nube que cubren cargas de trabajo de IaaS y SaaS en la nube. Las operaciones del proveedor están geográficamente diversificadas y sus clientes tienden a estar en el segmento del mercado intermedio. El año pasado, OpenText mejoró Data Protector al mejorar el soporte para SAP HANA, control de acceso basado en roles (RBAC), MongoDB y deduplicación. Data Protector para cargas de trabajo en la nube agregó soporte de VM para Azure Cloud, Azure Stack HCI, Google Cloud y Virtuozzo, y mejoró las integraciones de exportación y API para Microsoft 365.

Puntos fuertes

- Precios basados en la capacidad: OpenText ha mejorado su modelo de licencia al simplificar un gran número de SKU en un único número de pieza basado en la capacidad. Este enfoque ofrece a los clientes una opción de gastos operativos fácilmente comprensible para entrar en un modelo de precios de pago por uso basado en la capacidad.

- Soporte tradicional para centros de datos empresariales: Data Protector tiene amplias capacidades de copia de seguridad de centros de datos. Admite un gran número de cargas de trabajo con un costo total de propiedad bajo en comparación con otros proveedores.

- Amplia compatibilidad con destinos de almacenamiento: Data Protector admite una amplia gama de dispositivos de copia de seguridad diseñados específicamente, múltiples protocolos de almacenamiento y bibliotecas de cintas.

Precauciones

- Carece de detección de anomalías y malware: Data Protector se queda significativamente atrás con respecto a otros proveedores en las capacidades de detección de malware y anomalías de ransomware. Estas capacidades están en el ecosistema OpenText, pero aún no se han integrado en Data Protector.

- Integración de producto principal: Para cubrir una gama completa de cargas de trabajo en centros de datos y en la nube se necesitan dos productos independientes: Data Protector y Data Protector for Cloud Workloads, que carecen de integración significativa.

- Posicionamiento poco claro del producto: En este momento, no está claro si la tecnología del producto estará totalmente integrada en la cartera de OpenText más amplia o si continuará como un producto independiente.

Rubrik

Rubrik es Líder en este Magic Quadrant. Su cartera de productos de copia de seguridad consta de Rubrik Security Cloud, que incluye múltiples ofertas de copia de seguridad, seguridad de datos y recuperación avanzada. Las operaciones de Rubrik están geográficamente diversificadas, y sus clientes son empresas grandes en su mayoría. Durante el periodo de evaluación, Rubrik introdujo múltiples capacidades nuevas o mejoradas. Estas incluyen un nuevo modelo de aprendizaje automático para la detección de ransomware, soporte para la detección de ransomware en los hipervisores Nutanix y Microsoft, recuperación mejorada para entornos VMware, un centro de comando de seguridad de datos que ayuda a las organizaciones a evaluar su postura de seguridad general y funciones de contención de amenazas para aislar malware en copias de seguridad.

Puntos fuertes

- Innovación en estrategia de productos, precios, marca y agrupación: Rubrik es innovador en su enfoque para ampliar sus ofertas centradas en la seguridad en torno a la copia de seguridad y la recuperación al proporcionar nuevas opciones de precios con niveles de usuario competitivos y basados en las capacidades para Microsoft 365, y simplificar su marca y agrupación de paquetes de productos.

- Funciones de protección y recuperación de ransomware: Rubrik tiene una oferta de productos completa y segura que protege el sistema y los datos de copia de seguridad contra ciberataques, incluye capacidades para detectar anomalías y malware dentro de los datos de las copias de seguridad y proporciona funciones de recuperación eficientes.

- Adopción empresarial: Las capacidades de ampliación y la asistencia al cliente diferenciada de Rubrik siguen atrayendo a grandes organizaciones empresariales, sustituyendo a una variedad de soluciones competitivas diferentes.

Precauciones

- Equilibrio de seguridad con copia de seguridad: Algunos clientes han expresado su preocupación por la capacidad de Rubrik para equilibrar sus iniciativas de oferta de seguridad de datos mientras mantiene el enfoque en los requisitos de los mercados emergentes para la copia de seguridad.

- Cobertura limitada de aplicaciones SaaS: Rubrik tiene un soporte limitado para aplicaciones SaaS más allá de Microsoft 365. La cobertura aún no está disponible para aplicaciones como Salesforce, Google Workspace, Microsoft Dynamics 365, Azure AD, ServiceNow, Azure DevOps y GitHub.

- Ofertas de almacenamiento en la nube limitadas gestionadas por el proveedor: Rubrik solo ofrece almacenamiento de Azure para sus soluciones de bóveda gestionadas por proveedores y BaaS.

Unitrends

Unitrends, una empresa de Kaseya, es un Especialista en este Magic Quadrant. Su cartera de copias de seguridad consiste en el software Unitrends Backup, Recovery Series Backup Appliance y

Spanning Backup para copias de seguridad de aplicaciones SaaS. Las operaciones del proveedor están geográficamente diversificadas y sus clientes tienden a estar en el segmento del mercado intermedio. En los últimos 12 meses, Unitrends presentó una oferta de BaaS para la copia de seguridad y recuperación ante desastres de Microsoft Azure VM. Unitrends también automatizó la administración de licencias para la copia de seguridad de Microsoft 365 a través de Azure AD Security Groups, y mejoró la seguridad de Unitrends con autenticación de dos factores a través de UniView. Además, Unitrends continúa ampliando la integración de UniView con otros productos de infraestructura y gestión de seguridad de Kaseya.

Puntos fuertes

- Administración unificada: Unitrends UniView ofrece acceso administrativo único a todos los componentes de la solución, incluidas la gestión de dispositivos, la copia de seguridad de terminales y las aplicaciones SaaS.
- Cartera completa: Unitrends continúa ampliando sus ofertas de software y dispositivos con la incorporación de servicios integrados de recuperación ante desastres en la nube.
- Integración de Kaseya: Unitrends continúa centrando la integración en la cartera de productos Kaseya IT Complete. Esto agilizará el acceso a recursos técnicos, de facturación y de soporte, y proporcionará más funciones a sus clientes.

Precauciones

- Idoneidad empresarial limitada: Con su enfoque en los mercados de pymes y empresas medianas, las iniciativas de crecimiento de Unitrends y la escalabilidad limitada de los dispositivos contribuyen a reducir la idoneidad para las cuentas de grandes empresas.
- Capacidades multinube limitadas: Unitrends Backup para Microsoft Azure solo admite Azure VM y carece de soporte para otras cargas de trabajo en Azure, como Azure SQL y Azure Blob. La expansión para brindar soporte a otros proveedores de nube, como AWS y GCP, está en curso.
- Estrategia de BaaS limitada: Unitrends se queda atrás con respecto a otros actores importantes cuyas soluciones BaaS gestionadas por proveedores admiten múltiples cargas de trabajo en la nube y en entornos locales, y otras aplicaciones SaaS, como Azure AD, ServiceNow y Microsoft Dynamics 365.

Veeam

Veeam es Líder en este Magic Quadrant. Su cartera de copias de seguridad está compuesta por Veeam Data Platform, que está compuesta por Veeam Backup & Replication, Veeam ONE y Veeam Recovery Orchestrator.

Las operaciones de Veeam están geográficamente diversificadas y sus clientes tienden a estar en el segmento de empresa, mercado intermedio y pymes. En los últimos 12 meses, Veeam lanzó 24

actualizaciones de productos, incluida Veeam v12, que contiene varias características nuevas como almacenamiento directo al objeto, inmutabilidad para Azure, protección NAS mejorada e integración más profunda con Kasten. Veeam también introdujo nuevos paquetes de precios que contienen nuevas combinaciones de sus productos de plataforma de datos.

Puntos fuertes

- Base de clientes fieles y satisfechos: El crecimiento y la retención de clientes de Veeam, y el nivel de participación de sus clientes en comunidades de grupos de usuarios y foros como Veeam Community, indican una base de clientes fieles y satisfechos.
- Soporte híbrido y multinube: La plataforma de datos Veeam está disponible para los tres principales proveedores de nube pública, donde ofrece una experiencia de recuperación híbrida, multinube y entre nubes coherente para las cargas de trabajo más utilizadas.
- Amplia red de socios y MSP: Las ofertas de Veeam están disponibles a través de una amplia red global de socios autorizados. Esto incluye reventa, alianza, implementación y socios MSP.

Precauciones

- Respuesta lenta a las tendencias clave del mercado: Veeam ha reaccionado lentamente a las tendencias clave del mercado y a las expectativas de los clientes a la hora de ofrecer servicios alojados por proveedores, como BaaS, plano de control basado en SaaS y bóvedas de almacenamiento, y capacidades nativas de detección de anomalías de ransomware basadas en análisis de datos.
- Complejidad general: Algunos clientes de Gartner indican que Veeam puede ser más complejo de gestionar a medida que aumenta el tamaño del entorno de copia de seguridad. Esto incluye la implementación de agentes Veeam separados por entorno protegido, la gestión de múltiples proxis de copia de seguridad y almacenamiento, y la selección y gestión adecuadas de la infraestructura de computación y almacenamiento para alinearse con los requisitos de rendimiento y almacenamiento.
- Protección por requisito de implementación: La implementación de una plataforma de datos Veeam segura requiere que los clientes diseñen, configuren y administren cuidadosamente la implementación para mitigar las amenazas cibernéticas, integrando la inmutabilidad y detección de ransomware proporcionadas por soluciones de terceros.

Veritas

Veritas es Líder en este Magic Quadrant. Su cartera de productos de copia de seguridad consta de NetBackup, NetBackup Appliances y Backup Exec, y sus ofertas en la nube de Veritas Alta, que incluyen Alta View, Alta BaaS, Alta Data Protection, Alta Recovery Vault y Alta SaaS Protection. Las operaciones de Veritas se encuentran geográficamente diversificadas. Sus clientes tienden a ser grandes empresas y tienen cierta presencia en el mercado intermedio. En los últimos 12 meses,

introdujo sus ofertas de Alta Cloud, incluidos su plano de control SaaS basado en la nube, BaaS y soporte ampliado de aplicaciones SaaS para incluir Salesforce y copia de seguridad de Google Workspace. NetBackup ha añadido compatibilidad con 13 nuevas cargas de trabajo de PaaS de bases de datos, recuperación aislada en dispositivos Flex Scale, análisis de malware de inmutabilidad NAS y GCP.

Puntos fuertes

- Opciones integrales de copia de seguridad y gestión: Las ofertas en la nube de Veritas Alta, combinadas con las capacidades del software NetBackup y sus dispositivos de hardware escalables y ampliables, proporcionan a los clientes empresariales una cartera integral de capacidades de copia de seguridad y recuperación, y múltiples opciones de implementación y gestión.

- Arquitectura nativa de la nube: Los servicios NetBackup y Alta se ejecutan en clústeres de Kubernetes que se ejecutan de forma nativa en Azure, AWS y GCP. En este diseño, los servicios de plano de datos funcionan independientemente del plano de gestión para ofrecer una arquitectura multinube elástica e inherentemente flexible.

- Amplia cobertura geográfica: Veritas y sus socios pueden vender, implementar y brindar soporte a las soluciones de Veritas en todas las geografías principales. Esto facilita a los clientes con responsabilidades en todo el mundo encontrar una solución de copia de seguridad que cumpla con sus requisitos técnicos y empresariales.

Precauciones

- Algunos productos en la nube son nuevos en el mercado: Las nuevas ofertas de gestión basadas en SaaS Alta BaaS y Alta View de Veritas son nuevas en el mercado. Hay pocos datos disponibles sobre la adopción del mercado o la satisfacción del cliente, lo que requiere una prueba de concepto (proof of concept, POC) integral para determinar los niveles de experiencia del cliente en la incorporación y el rendimiento.

- Estrategia de productos y servicios centrada en la empresa: El enfoque principal de Veritas se centra en grandes clientes empresariales en su estrategia de productos y servicios Alta y NetBackup, lo que hace que sea potencialmente menos adecuado para clientes medianos, comerciales y pymes.

- Soporte de aplicaciones SaaS menos completo: Veritas se queda atrás con respecto a otros proveedores en el soporte de otras aplicaciones SaaS como Microsoft Azure AD, Azure DevOps, Microsoft Dynamics 365 y GitHub con Alta BaaS.

Proveedores añadidos y eliminados

Revisamos y ajustamos nuestros criterios de inclusión para los Magic Quadrants a medida que los mercados cambian. Como resultado de estos ajustes, la combinación de proveedores en cualquier

Magic Quadrant puede cambiar con el tiempo. La aparición de un proveedor en un Magic Quadrant un año y no en el siguiente no indica necesariamente que hayamos cambiado nuestra opinión sobre ese proveedor. Puede ser un reflejo de un cambio en el mercado y, por lo tanto, un cambio en los criterios de evaluación, o de un cambio de enfoque por parte de ese proveedor.

Añadido

Microsoft: este proveedor cumplió los criterios de inclusión de este año.

OpenText: este proveedor se incluyó en el Magic Quadrant de este año tras completar la adquisición de Micro Focus en enero de 2023.

Eliminado

Zerto, una empresa de HPE: este proveedor no cumplió los criterios de inclusión de este año.

Criterios de inclusión y exclusión

Los siguientes criterios representan los atributos específicos que los analistas creen que son necesarios para la inclusión en esta investigación:

- El proveedor debe cumplir al menos uno de los siguientes criterios de ingresos. Los ingresos deben derivarse únicamente de su cartera de productos de copia de seguridad y recuperación. Estos ingresos no deben incluir ingresos generados por servicios de implementación, de alojamiento de servidores BaaS u ofertas de proveedores de servicios gestionados.
    - El proveedor debe haber generado ingresos por licencias (perpetuas o por suscripción) y mantenimiento (principios contables generalmente aceptados [generally accepted accounting principles, GAAP]) de más de 50 millones de USD en los últimos cuatro trimestres que finalizan el 28 de febrero de 2023 (o)
    - El proveedor debe haber generado licencias (perpetuas o por suscripción) e ingresos por mantenimiento (GAAP) de más de 25 millones de USD, combinados con una tasa de crecimiento interanual del 20 %, durante los últimos cuatro trimestres que finalizan el 28 de febrero de 2023.
- Las soluciones de copia de seguridad y recuperación cualificadas del proveedor deben venderse y comercializarse principalmente entre organizaciones empresariales grandes y del mercado intermedio superior. Gartner define el mercado intermedio superior como el que cuenta con 500 a 999 empleados, y la empresa grande como aquella que cuenta con 1000 empleados o más.
- La solución de copia de seguridad y recuperación cualificada del proveedor debe centrarse en proteger a los clientes empresariales que operan en entornos híbridos/multinube, que incluyen entornos de centros de datos (centro de datos tradicional o instalación de colocación) y cargas de

trabajo de IaaS y PaaS basadas en la nube. La protección de sitios remotos se considera una extensión de estas capacidades básicas.

- Los nuevos productos o actualizaciones de los productos existentes que se lanzaron en los últimos 12 meses deben estar disponibles en general el 31 de marzo de 2023 o antes para ser considerados para su evaluación. Todos los componentes deben estar disponibles al público, enviarse e incluirse en la lista de precios publicada del proveedor a partir de esta fecha. Los productos que se envíen después de esta fecha solo influirán en el eje Integridad de la visión.

- El proveedor debe vender y apoyar activamente sus productos de copia de seguridad y recuperación bajo su propio nombre comercial en al menos tres de las siguientes zonas geográficas principales: Norteamérica, EMEA, Asia/Pacífico y Sudamérica. Al menos el 25 % de los ingresos totales deben provenir de fuera de su geografía principal.

- El proveedor debe prestar servicios a una base instalada de al menos 1000 clientes dentro del mercado, según se define en la Definición o descripción del mercado. Además, al menos 250 de los 1000 clientes deben haber implementado la solución de copia de seguridad para un mínimo de 100 servidores físicos o 300 servidores virtuales en un único sitio de implementación o región de la nube. Esto excluye las copias de seguridad de terminales.

- El producto debe instalarse en al menos tres de las siguientes zonas geográficas principales (Norteamérica, EMEA, Asia/Pacífico y Sudamérica). El proveedor proporcionará pruebas de un mínimo de 50 clientes de producción que obtengan ingresos en cada una de las tres zonas geográficas.

- El proveedor debe emplear al menos 100 empleados a tiempo completo en funciones de ingeniería, ventas y marketing combinadas a 31 de marzo de 2023.

- El proveedor debe tener al menos una solución de copia de seguridad y recuperación cualificada disponible comercialmente para su uso por parte de las empresas durante tres años naturales antes del 1 de marzo de 2023, es decir, debe haber estado disponible comercialmente al menos a partir del 1 de marzo de 2020.

- El producto puede venderse como una oferta solo de software, como almacenamiento de copia de seguridad integrado o dispositivo virtualizado (aplicación de copia de seguridad más almacenamiento de copia de seguridad en una única oferta integrada) o como una oferta BaaS basada en SaaS y desarrollada por el proveedor.

Se aplican los siguientes criterios de exclusión:

- Proveedores que ofrecen productos o soluciones cuyo software se obtiene principalmente de un ISV externo.

- Productos que sirven solo como objetivo o destino para la copia de seguridad, pero que no realizan realmente la función de gestión de copia de seguridad y restauración. Entre los ejemplos se incluyen dispositivos de deduplicación diseñados específicamente, red de área de almacenamiento (SAN), NAS o almacenamiento de objetos.
- Proveedores que hacen copias de seguridad directamente en la nube pública sin almacenar una copia local en las instalaciones.
- Proveedores cuya fuente principal de ingresos por productos (más del 75 % de los ingresos totales) proviene de alojamientos de centros de datos y proveedores de servicios gestionados.
- Productos o soluciones diseñados y posicionados principalmente como soluciones para realizar copias de seguridad de terminales como computadoras portátiles y de escritorio y dispositivos móviles.
- Productos o soluciones diseñados y posicionados principalmente como soluciones para hacer copias de seguridad de aplicaciones SaaS.
- Productos o soluciones diseñados y posicionados principalmente como soluciones para respaldar oficinas remotas, ubicaciones periféricas y entornos de mercado intermedio/pyme inferior.
- Productos o soluciones diseñados y posicionados principalmente como soluciones para entornos homogéneos, como herramientas diseñadas para hacer copias de seguridad solo de AWS EC2, Azure Virtual Machines, Microsoft Hyper-V, VMware, Red Hat o contenedores.
- Productos o soluciones diseñados para realizar copias de seguridad de proveedores de sistemas de almacenamiento o hiperconvergentes específicos.
- Productos que sirven solo como herramientas de replicación y recuperación ante desastres.
- Productos que sirven principalmente para gestionar las capacidades de instantánea y replicación de matrices de almacenamiento.
- Productos que se posicionan principalmente para la gestión de datos de copia (copy data management, CDM) o pruebas DevOps.
- Productos posicionados principalmente para la protección continua de datos (continuous data protection, CDP).

Criterios de evaluación

Capacidad de ejecución

Tabla 1: Capacidad para ejecutar criterios de evaluación

Criterios de evaluación	*Ponderación*
Producto o servicio	Elevado
Viabilidad general	Elevado
Ejecución de ventas y precios	Medio
Registro y capacidad de respuesta del mercado	Elevado
Ejecución de marketing	Bajo
Experiencia del cliente	Elevado
Operaciones	Sin calificar

Fuente: Gartner (agosto de 2023)

Integridad de la visión

Tabla 2: Criterios de evaluación de la Integridad de la visión

Criterios de evaluación	*Ponderación*
Comprensión del mercado	Elevado
Estrategia de marketing	Medio
Estrategia de ventas	Medio

Criterios de evaluación	*Ponderación*
Estrategia de oferta (producto)	Elevado
Modelo de negocio	Medio
Estrategia vertical o industrial	Medio
Innovación	Elevado
Estrategia geográfica	Medio

Fuente: Gartner (agosto de 2023)

Descripciones del cuadrante

Líderes

Los Líderes tienen las medidas combinadas más altas de Capacidad de ejecución e Integridad de la visión. Tienen las carteras de productos más completas y escalables para cumplir con los requisitos de protección de datos de entornos de TI híbridos y multinube. Tienen un historial probado de presencia en el mercado y rendimiento financiero establecidos. Para su visión, se perciben en el sector como líderes de pensamiento y creadores de propiedad intelectual (PI), y tienen planes bien articulados para mejorar las capacidades de recuperación, mejorar la facilidad de implementación y administración, y aumentar su escalabilidad y amplitud de producto. Una piedra angular para los Líderes es la capacidad de articular cómo se abordarán los nuevos requisitos como parte de su visión para la gestión de la recuperación.

Como grupo, se puede esperar que los Líderes se consideren como parte de la mayoría de las nuevas propuestas de compra y que tengan altos índices de éxito para ganar nuevos negocios. Sin embargo, una gran cuota de mercado por sí sola no es un indicador principal de un Líder. Los Líderes son proveedores estratégicos que están bien posicionados para el futuro, y establecieron el éxito al satisfacer las necesidades de los centros de datos de empresas grandes y de gama media/alta.

Contendientes

Los Contendientes pueden operar hoy, pero pueden tener una visión más limitada que los Líderes, o aún no han producido o comercializado completamente su visión. Tienen productos capaces y pueden funcionar bien para muchas empresas. Estos proveedores tienen los recursos financieros y del mercado y las capacidades para convertirse potencialmente en Líderes. Sin embargo, la pregunta importante es si comprenden las tendencias del mercado y los requisitos del mercado para tener éxito en el futuro, y si pueden mantener su impulso al operar a un alto nivel con el tiempo.

Un Contendiente puede tener una sólida cartera de respaldo. Sin embargo, es posible que no haya podido aprovechar plenamente sus oportunidades o que no tenga la misma capacidad que los Líderes para influir en las expectativas del usuario final o ser considerado para implementaciones sustancialmente más amplias. Los Contendientes no pueden competir agresivamente fuera de su base de cuentas existente y pueden centrarse principalmente en la retención. Es posible que estos proveedores no dediquen suficientes recursos de desarrollo a entregar productos con un amplio atractivo de la industria y características diferenciadas de manera oportuna. Es posible que no comercialicen eficazmente sus capacidades o exploten por completo suficientes recursos de campo para dar lugar a una mayor presencia en el mercado.

Visionarios

Los Visionarios tienen visión de futuro y promueven sus capacidades de cartera hacia adelante o muy por delante del mercado, pero su operación general no los ha impulsado a ser Contendientes o Líderes. A menudo, esto se debe a ventas y marketing limitados, y a veces se debe a la escalabilidad, el alcance de las cargas de trabajo protegidas o la amplitud de la funcionalidad o el soporte de la plataforma. Estos proveedores se diferencian principalmente por la innovación de productos y los beneficios percibidos por el cliente. Sin embargo, aún no han logrado la integridad de la solución ni han mantenido amplias ventas y marketing. No han logrado el éxito en la presencia ni han demostrado las implementaciones continuas y exitosas de grandes empresas necesarias para darles la visibilidad superior de los Líderes.

Algunos proveedores salen del cuadrante de los Visionarios y pasan al cuadrante de los Especialistas porque su tecnología ya no es visionaria (es decir, la competencia los alcanzó). En algunos casos, no han podido establecer una presencia en el mercado que justifique pasar a los cuadrantes de los Contendientes o de los Líderes, o incluso permanecer en el cuadrante de los Visionarios.

Especialistas

Es importante tener en cuenta que Gartner no recomienda eliminar a los Especialistas de las evaluaciones de los clientes. Los Especialistas se centran específica y conscientemente en un subsegmento del mercado general, u ofrecen capacidades relativamente amplias sin una gran escala empresarial o el éxito general de los competidores en otros cuadrantes. En varios casos, los Especialistas son muy fuertes en el segmento de empresas de gama media/alta. También venden de

forma oportunista a grandes empresas, pero con ofertas y servicios generales que, en la actualidad, no son tan completos como los de otros proveedores centrados en el mercado de grandes empresas.

Los Especialistas pueden centrarse en zonas geográficas o mercados verticales específicos, o en una implementación de copia de seguridad o un servicio de caso de uso específicos; o simplemente pueden tener horizontes modestos o capacidades generales más bajas en comparación con la competencia. Otros Especialistas son demasiado nuevos en el mercado o se han quedado atrás y, aunque vale la pena verlos, aún no han desarrollado completamente la funcionalidad completa o han demostrado de forma coherente una visión amplia o la Capacidad de ejecución.

Contexto

Los líderes de infraestructura y operaciones (I&O) encargados de las operaciones de la copia de seguridad deben evaluar y reestructurar la infraestructura de la copia de seguridad para incluir los siguientes aspectos de tecnología, operaciones y consumo:

- Invertir en soluciones para la copia de seguridad que aborden los requisitos de protección de los datos en los entornos de centros de datos, híbridos, multinube y periféricos. Favorecer soluciones que ofrezcan un único panel de vidrio para gestionar estos entornos distribuidos.
- Elegir soluciones para la copia de seguridad que proporcionen una oferta integrada o incorporada para proteger los datos de la copia de seguridad de un ataque de ransomware, detección de malware y anomalías de ransomware, y capacidades de recuperación acelerada de ataques de ransomware.
- Comprender a fondo el nivel de resistencia proporcionado en la copia de seguridad principal y la necesidad de invertir en copias de seguridad adicionales para garantizar la resiliencia de la copia de seguridad, como la nube, el bloqueo de objetos compatible, las bóvedas de datos inmutables o la cinta.
- Elegir productos que ofrezcan capacidades de pruebas de recuperación seguras y granulares.
- Alinear la arquitectura de la copia de seguridad con las necesidades de recuperación operativa de la organización. Optimizar el uso del almacenamiento de copias de seguridad mediante el uso de almacenamiento basado en el disco, como dispositivos de copia de seguridad diseñados específicamente o almacenamiento SAN, de objetos o de sistemas de archivos distribuidos para la recuperación operativa, y el uso de cinta en entornos locales o almacenamiento de objetos, o almacenamiento en la nube pública o alojado por el proveedor para las copias de retención y de espacio de aire a largo plazo.
- Determinar el costo total de propiedad a largo plazo de pasar de las licencias perpetuas a los modelos de licencias por suscripción. Para las suscripciones, comprender las implicaciones de los

costos de los pagos anualizados frente a los pagos por adelantado y de dar de baja la suscripción antes de que finalice el plazo.
- Comprender las implicaciones de los costos a largo plazo de varios modelos de precios ofrecidos por los proveedores: basado en VM, basado en sockets, basado en nodos, basado en universales, TB de front-end, TB de back-end y basado en agentes. Invertir en el modelo adecuado basado en la hoja de ruta de la aplicación y la infraestructura de la organización.

- Seleccionar proveedores que admitan la organización por niveles de las copias de seguridad para la nube pública y en la nube pública para ahorrar en costos de almacenamiento de copias de seguridad. Elegir soluciones que admitan la recuperación de aplicaciones a partir de copias de seguridad en la nube pública para abordar casos de uso de recuperación, prueba/desarrollo o recuperación ante desastres (DR) de ransomware.

- Seleccionar proveedores que puedan aumentar el valor de los datos de la copia de seguridad más allá de los eventos de recuperación. Priorizar las soluciones que ofrecen análisis de datos confidenciales y descubrimiento electrónico, aborden los requisitos de cumplimiento, respalden el análisis y otros enriquecimientos de datos, reutilicen los datos de respaldo para pruebas/desarrollo y proporcionen capacidades complementarias como DR.

Descripción general del mercado

El mercado de software de copia de seguridad y recuperación empresarial ha experimentado una transformación significativa en los últimos dos años. Los proveedores de copias de seguridad evaluados en este Magic Quadrant se centran principalmente en las siguientes áreas:

- Plano de control centralizado: A medida que las empresas avanzan hacia un modelo de TI híbrido y multinube, y las cargas de trabajo se distribuyen en todo el centro de datos, la nube pública y la periferia, proteger estas cargas de trabajo, independientemente de la ubicación, es fundamental. Los principales proveedores de copias de seguridad están abordando esto ofreciendo una plataforma de gestión que puede implementarse en la nube pública, en el centro de datos principal o, cada vez más, como un servicio alojado en la nube pública.

- Protección multinube: A medida que las organizaciones implementan aplicaciones y cargas de trabajo en múltiples entornos de nube, el requisito de que las soluciones se integren y protejan los entornos multinube es ahora más crítico. La flexibilidad para elegir qué proveedor de nube se utiliza para almacenar los datos de la copia de seguridad es ideal.

- Resistencia al ransomware: El aumento del número de ataques de ransomware ha dado lugar a que los proveedores tomen medidas concretas para avanzar en una infraestructura de copia de seguridad resistente. La mayoría de los proveedores pretenden hacer que el repositorio de copias de seguridad principal sea más resistente al admitir el almacenamiento inmutable para las primeras copias. Aunque la mayoría de los proveedores admiten la creación de segundas copias inmutables de copias de seguridad a través del almacenamiento “escribir una vez, leer muchas” (write once, read many, WORM) habilitado, como el bloqueo de almacenamiento de objetos, los

principales proveedores de copias de seguridad han introducido bóvedas de datos inmutables en entornos locales, en la nube y alojadas por el proveedor.

- Detección y corrección de ransomware: Los principales proveedores han creado capacidades para detectar ataques de ransomware mediante la supervisión de anomalías de comportamiento de los datos protegidos y están añadiendo detección de malware proporcionada mediante la asociación con proveedores de seguridad o mediante el desarrollo interno de estas capacidades. La mayoría de los proveedores también tienen como objetivo simplificar el proceso de recuperación de ransomware acelerando la identificación del mejor y más limpio punto de recuperación, creando puntos de recuperación seleccionados, que combinan múltiples puntos de recuperación y creando un entorno de prueba y recuperación aislado.

- Ofertas de BaaS: Los principales proveedores de copias de seguridad están ampliando las capacidades de BaaS para incluir entornos locales, IaaS, PaaS y SaaS. Aunque generalmente no sustituyen las implementaciones de copias de seguridad en entornos locales, los clientes de Gartner están invirtiendo en ofertas de BaaS para complementar estas implementaciones a fin de simplificar la protección de entornos, incluidas cargas de trabajo en entornos locales seleccionados, y en la nube periférica y pública.

- Uso de inteligencia artificial y aprendizaje automático: Los principales proveedores han introducido algoritmos basados en la inteligencia artificial/el aprendizaje automático (AI/ML) en las capacidades de detección de anomalías de ransomware y para mejorar las prácticas de asistencia al cliente. Las capacidades más recientes incluyen avances en la clasificación automatizada de datos y actividades administrativas basadas en conversaciones.

- Compatibilidad con copias de seguridad de IaaS y PaaS en la nube pública: La mayoría de los proveedores de copias de seguridad en entornos locales han aumentado su inversión para ampliar las capacidades a fin de proteger las cargas de trabajo nativas de la nube, especialmente las máquinas virtuales y las aplicaciones alojadas en AWS, Microsoft Azure y Google Cloud Platform. Los principales proveedores de copias de seguridad están ampliando el soporte de copias de seguridad de productos DBaaS como Amazon RDS, Amazon Aurora y Microsoft Azure SQL. Algunos proveedores integran su software de copia de seguridad con las capacidades de instantánea nativas que ofrecen estos proveedores de la nube; otros continúan reutilizando su software de copia de seguridad existente “tal cual” en la nube para proporcionar copias de seguridad basadas en agentes de las aplicaciones alojadas en la nube.

- Compatibilidad con aplicaciones basadas en SaaS: Los líderes de I&O han comenzado a incluir aplicaciones SaaS como Microsoft 365, Google G Suite y Salesforce como parte de su estrategia de copia de seguridad. La mayoría de los proveedores evaluados en esta investigación admiten copias de seguridad de Microsoft 365 y Salesforce a través de socios o desarrollaron estas capacidades internamente. Los principales proveedores protegen otras aplicaciones SaaS, como Microsoft Azure Active Directory, Microsoft Dynamics 365, Microsoft Power Apps, Atlassian y ServiceNow.

- Organización por niveles para la nube pública: La mayoría de los proveedores evaluados en este Magic Quadrant admiten la organización por niveles de los datos de la copia de seguridad para la nube pública. Esto reduce los costos de almacenamiento de copias de seguridad en entornos locales. Los destinos de almacenamiento en la nube pública más comúnmente admitidos son Amazon Simple Storage Service (Amazon S3) y Azure Blob Storage. En la mayoría de los casos, los datos de la copia de seguridad se autodescriben, lo que significa que si se pierden los datos y el catálogo en entornos locales, se puede volver a instalar una instancia del software de copia de seguridad en la nube y se pueden restaurar los datos. Algunos proveedores también se integran con las políticas del ciclo de vida de los proveedores de nube (por ejemplo, la migración de datos de Amazon S3 a Glacier o el almacenamiento de Azure Blob a Azure Archive Blob).

- Recuperación en la nube pública: Hoy en día, los principales proveedores de copias de seguridad admiten la restauración de los datos de las copias de seguridad a servidores en la nube pública. Una instancia del software de la copia de seguridad se puede instalar en la nube pública y los datos de la copia de seguridad se pueden restaurar a una instancia de computación en la nube pública. Esto proporciona una rápida recuperación operativa si el entorno local no está disponible. Los datos de la copia de seguridad también se pueden utilizar con fines de prueba/desarrollo en la nube pública.

- Copia de seguridad de la base de datos NoSQL: Las empresas tradicionales siguen ejecutando sus aplicaciones empresariales principales en bases de datos de sistemas de gestión de bases de datos relacionales (relational database management system, RDMS), como Oracle y Microsoft SQL. Sin embargo, los proyectos de Mode 2, como datos masivos, suelen aprovechar bases de datos NoSQL como MongoDB y Cassandra. A medida que estos proyectos comienzan a escalarse y ofrecen valor tangible, existe una creciente necesidad de proteger esos entornos. Proveedores establecidos como Commvault, Dell Technologies y Veritas han comenzado a abordar estos requisitos de la copia de seguridad al incorporar esas capacidades de forma nativa en la plataforma de la copia de seguridad. Proveedores como Rubrik y Cohesity han realizado adquisiciones estratégicas en este espacio.

- Recuperación instantánea de bases de datos, máquinas virtuales y sistemas de archivos: La mayoría de los proveedores admiten la recuperación instantánea de máquinas virtuales (VM) mediante el montaje de la VM de la copia de seguridad directamente en el host de producción a través de NFS. Las VM pueden estar disponibles al instante, mientras que el proceso de recuperación real puede iniciarse en segundo plano. Proveedores como Cohesity y Rubrik ofrecen la recuperación instantánea de las bases de datos como Microsoft SQL y Oracle, mientras que Veeam también ofrece el acceso a archivos compartidos en un momento determinado desde las copias de seguridad a través de archivos compartidos SMB de solo lectura.

- Copia de seguridad del contenedor: Los principales proveedores anunciaron el soporte para la copia de seguridad de contenedores, ya sea mediante la creación de estas capacidades de forma nativa en su plataforma existente o a través de adquisiciones. Si bien las consultas de los clientes

de Gartner muestran poco interés por la copia de seguridad de contenedores, prevemos que aumentará su adopción a medida que se implementen más contenedores que utilicen almacenamiento persistente para soportar las cargas de trabajo de producción.
- Modelos de licencia: Aunque algunas opciones de licencias perpetuas siguen disponibles, todos los principales proveedores de este mercado han hecho la transición para proporcionar sus ofertas de software a través de modelos de licencias basados en la suscripción. La mayoría de las ofertas de licencias basadas en la suscripción son acuerdos de varios años. Las licencias basadas en el consumo son una tendencia emergente para las licencias que proporciona la capacidad de otorgar una licencia a lo que se está utilizando en función de la medición a intervalos más frecuentes.

Definiciones de los criterios de evaluación

Capacidad de ejecución

Producto o servicio: Bienes y servicios básicos ofrecidos por el proveedor para el mercado definido. Esto incluye las capacidades actuales del producto o servicio, calidad, conjuntos de características, habilidades, etc., tanto si se ofrecen de forma nativa como a través de acuerdos o asociaciones de OEM según se establece en la definición del mercado y se detallan en los criterios secundarios.

Viabilidad general: La viabilidad incluye una evaluación del estado financiero general de la organización, el éxito financiero y práctico de la unidad de negocio, y la probabilidad de que la unidad de negocio individual continúe invirtiendo en el producto, continúe ofreciendo el producto y avance el estado de la tecnología dentro de la cartera de productos de la organización.

Ejecución de ventas y precios: Las capacidades del proveedor en todas las actividades de preventa y la estructura que las soporta. Esto incluye la gestión de acuerdos, la fijación de precios y la negociación, el soporte de preventa y la eficacia general del canal de ventas.

Registro y capacidad de respuesta del mercado: Capacidad para responder, cambiar de dirección, ser flexible y alcanzar el éxito competitivo a medida que se desarrollan oportunidades, los competidores actúan, las necesidades del cliente evolucionan y la dinámica del mercado cambia. Este criterio también tiene en cuenta el historial de la capacidad de respuesta del proveedor.

Ejecución de marketing: La claridad, calidad, creatividad y eficacia de los programas diseñados para transmitir el mensaje de la organización de modo de influir en el mercado, promover la marca y el negocio, aumentar la percepción de los productos y establecer una identificación positiva con el producto o la marca y la organización en la mente de los compradores. Esta “presencia” puede estar impulsada por una combinación de publicidad, iniciativas promocionales, liderazgo intelectual, publicidad verbal y actividades de ventas.

Experiencia del cliente: Relaciones, productos y servicios o programas que permiten a los clientes tener éxito con los productos evaluados. Concretamente, esto incluye las formas en que los clientes reciben soporte técnico o soporte de cuenta. Esto también puede incluir herramientas auxiliares,

programas de atención al cliente (y la calidad de estos), disponibilidad de grupos de usuarios, acuerdos de nivel de servicio, etc.

Operaciones: La capacidad de la organización para cumplir sus objetivos y compromisos. Los factores incluyen la calidad de la estructura organizacional, incluidos habilidades, experiencias, programas, sistemas y otros medios que permiten a la organización operar de forma eficaz y eficiente de manera continua.

Integridad de la visión

Comprensión del mercado: Capacidad del proveedor para comprender los deseos y las necesidades de los compradores y traducir estos elementos en productos y servicios. Los proveedores que muestran el mayor grado de visión escuchan y comprenden los deseos y las necesidades de los compradores, y pueden dar forma o mejorar esos elementos con su visión añadida.

Estrategia de marketing: Un conjunto de mensajes claro y diferenciado que se comunica de forma coherente en toda la organización y se externaliza a través del sitio web, la publicidad, los programas del cliente y las declaraciones de posicionamiento.

Estrategia de ventas: La estrategia para vender productos que utiliza la red adecuada de afiliadas de ventas directas e indirectas, marketing, servicio y comunicación que amplían el alcance y la profundidad de la magnitud del mercado, las habilidades, la experiencia, las tecnologías, los servicios y la base de clientes.

Estrategia de oferta (producto): El enfoque del proveedor para el desarrollo y entrega de productos que enfatiza la diferenciación, funcionalidad, metodología y conjuntos de características a medida que se asignan a los requisitos actuales y futuros.

Modelo de negocio: La solidez y lógica de la propuesta de negocio subyacente del proveedor.

Estrategia vertical o industrial: La estrategia del proveedor de orientar recursos, habilidades y ofertas para satisfacer las necesidades específicas de segmentos de mercado individuales, incluidos los mercados verticales.

Innovación: Disposiciones directas, relacionadas, complementarias y sinérgicas de recursos, experiencia o capital para fines de inversión, consolidación, defensivos o preventivos.

Estrategia geográfica: La estrategia del proveedor de orientar recursos, habilidades y ofertas para satisfacer las necesidades específicas de las geografías fuera de la geografía nativa, ya sea directamente o a través de socios, canales y subsidiarias, según corresponda para esa geografía y mercado.

Learn how Gartner can help you succeed.

Become a Client ↗

© 2023 Gartner, Inc. o sus afiliadas. Todos los derechos reservados. Gartner es una marca comercial registrada de Gartner, Inc. y sus afiliadas. Esta publicación no puede reproducirse ni distribuirse de ninguna forma sin el permiso previo por escrito de Gartner. Consta de las opiniones de la organización de investigación de Gartner, que no deben interpretarse como declaraciones de hechos. Aunque la información que se incluye en esta publicación se obtuvo de fuentes que se consideran confiables, Gartner se desliga de todas las garantías en cuanto a la exactitud, integridad o adecuación de dicha información. Aunque la investigación de Gartner puede abordar cuestiones legales y financieras, Gartner no proporciona asesoramiento legal o de inversión y su investigación no debe interpretarse ni utilizarse como tal. Su acceso y uso de esta publicación se rigen por la Política de uso de Gartner. Gartner se enorgullece de su reputación de independencia y objetividad. Su investigación es producida de forma independiente por su organización de investigación sin la aportación o influencia de ningún tercero. Para obtener más información, consulte "Principios rectores sobre independencia y objetividad". La investigación de Gartner no puede utilizarse como contribución para la capacitación o el desarrollo de inteligencia artificial generativa, aprendizaje automático, algoritmos, software o tecnologías relacionadas.

La Investigación de Gartner contenida en este documento se ha traducido de su original en inglés al idioma anterior/a continuación. Gartner ha realizado todos los esfuerzos comerciales razonables para garantizar que la traducción sea lo más precisa y completa posible. Sin embargo, al igual que con todas las traducciones, inevitablemente puede haber algún grado de discrepancia. En caso de discrepancia, en cuanto al contenido o la intención, siempre prevalecerá el significado que se establece en el inglés original.

Gartner

© 2023 Gartner, Inc. and/or its Affiliates. All Rights Reserved.