

Fecha de publicación:

25 de febrero de 2025

Autor(es):

Hollie Hennessy, analista principal

On the Radar: Acronis ofrece funciones de copia de seguridad y recuperación para la resiliencia y ciberseguridad de entornos de OT

Resumen

Catalizador

La oferta de tecnología operativa (OT) de Acronis se centra en el componente de la ciberseguridad que corresponde a la "recuperación". Proporciona copias de seguridad, recuperación y seguridad de los datos para entornos de OT con el fin de mejorar la resiliencia y la ciberseguridad. La sólida red de partners y canales de Acronis también consolida su reputación en el ámbito de la seguridad de entornos de OT.

Opinión de Omdia

La seguridad en entornos de OT incluye varios objetivos diferentes, uno de los cuales es la posibilidad de recuperar los sistemas y archivos afectados en caso de sufrir algún incidente o ataque. En entornos de infraestructuras operativas y críticas, quizá incluso en mayor medida que en algunos entornos de TI, la continuidad de la actividad empresarial es fundamental, dadas las exigencias normativas para muchas organizaciones con infraestructuras críticas y el gran impacto financiero o el daño potencial que suele causar el tiempo de inactividad.

Es vital contar con un plan de copia de seguridad y recuperación eficaz que se haya sometido a pruebas exhaustivas y cuya eficacia se haya podido demostrar en cualquier entorno. Incluso con la mejor protección, aún puede producirse un ataque. Por lo tanto, saber qué hacer en caso de que se produzca un incidente y poder volver a poner en marcha los sistemas en el plazo más breve posible debería ser una parte fundamental de cualquier estrategia de ciberseguridad. Las copias de seguridad periódicas son primordiales, así como disponer de un proceso para restaurar los datos sustraídos de forma rápida y eficaz.

Las soluciones de copia de seguridad y recuperación de Acronis se centran principalmente en el canal. Ofrecen a los proveedores de servicios y fabricantes industriales la oportunidad de integrar las funciones de copia de seguridad y recuperación de Acronis en sus propios servicios y plataformas, y además proporcionan un producto específico para empresas y organizaciones que operen sobre todo en entornos de OT.

¿Por qué debería tener en cuenta a Acronis?

Acronis se ha asociado con partners OEM, lo que le permite ofrecer su solución de copia de seguridad y recuperación a un gran número de proveedores líderes de automatización industrial en sectores como el de la fabricación, la sanidad y la energía. El producto del proveedor ayuda a garantizar el cumplimiento de los requisitos normativos (p. ej., la directiva NIS2) y de los estándares (como ISA/IEC 62443). Además, puede mejorar la oferta de productos de los proveedores de automatización industrial al proporcionar un servicio más sólido y fiable a sus clientes. Gracias a su experiencia en el ámbito de las copias de seguridad y la recuperación, Acronis ha podido desarrollar una solución que se adapta a las necesidades de los entornos industriales y los sistemas heredados que todavía se utilizan en ellos.

Contexto del mercado

El mercado de la seguridad de OT está dominado por la administración de recursos, la supervisión, la detección y la respuesta, y muchos de los proveedores líderes en este ámbito ofrecen funciones en todas o la mayoría de estas áreas. Dicho esto, en el mercado se requieren funciones adicionales para cumplir con los requisitos normativos y para satisfacer las necesidades de las organizaciones industriales y de aquellas que se centren en entornos de OT.

La continuidad de la actividad empresarial (ya sea por motivos de seguridad, operativos o financieros) es de suma importancia en estos entornos. Por lo tanto, es fundamental poder detectar posibles ataques o brechas de seguridad, así como prevenir las amenazas ya conocidas. Se han desarrollado funciones adicionales para abordar este último aspecto, ya sea mediante la automatización preventiva o enfoques más proactivos, como la gestión de riesgos y vulnerabilidades, la simulación de ataques y brechas de seguridad, y la gestión de la superficie de ataque.

Sin embargo, dado que ningún sistema es completamente infalible, es necesario poder recuperarse de cualquier incidente. Esta parte del mercado se centra en la ciberseguridad y la resiliencia, lo que incluye herramientas y servicios de respuesta ante incidentes, análisis forense, y recuperación de datos y sistemas, ámbitos en los que las soluciones de Acronis son una buena opción para los entornos de OT.

El marco de ciberseguridad del NIST (CSF) 2.0 es una buena indicación de los requisitos de ciberseguridad para organizaciones críticas (y, de hecho, para todas). Este marco, centrado inicialmente en las infraestructuras críticas, se ha adoptado y citado en tal medida que su ámbito de aplicación se ha ampliado a más tipos de infraestructuras. La versión actualizada del marco abarca diversas funciones:

- Identificación
- Protección
- Detección
- Respuesta
- Recuperación
- Administración (su última incorporación)

Descripción del producto/servicio

Las funciones de protección de datos de Acronis abarcan ampliamente dos áreas, "Backup" (Copia de seguridad) y "Disaster Recovery" (Recuperación ante desastres), que forman parte de su plataforma, Acronis Cyber Protect Entre las funciones que se incluyen se encuentran las siguientes:

- Copia de seguridad de la imagen del disco completo en un sistema en ejecución, con aplicación de parches a prueba de fallos, que crea una copia de seguridad de la imagen antes de aplicar los parches en los sistemas o en las aplicaciones en cuestión.
- Autoservicio con "One Click Recovery".
- Restauración universal, que permite recuperar cualquier hardware o hipervisor.
- Restauración instantánea, que permite llevar a cabo arranques y ejecuciones mientras se efectúa la restauración.
- Copias de seguridad inmutables para reforzar la seguridad.
- Compatibilidad con Windows, Linux y otros sistemas operativos y aplicaciones, incluidas versiones antiguas como Windows XP que todavía se utilizan en entornos industriales.
- Análisis antimalware y actualizaciones de antivirus automatizadas dentro del proceso de recuperación.
- Recuperación ante desastres totalmente integrada como servicio.

Diseñada para entornos de OT, la solución de Acronis Cyber Protect realiza instalaciones y copias de seguridad en tiempo real, por lo que no es necesario desconectar los sistemas ni reiniciarlos. Además, la solución de Acronis admite la recuperación en nuevo hardware si fuera necesario. Esto se lleva a cabo mediante el agente de Acronis Cyber Protect, que se puede instalar con componentes antimalware o sin ellos, en función de las restricciones y requisitos de cada cliente.

El proceso de recuperación se simplifica gracias a One Click Recovery, lo que significa que las personas que no sean profesionales de TI o de seguridad pueden volver a poner en marcha los sistemas sin necesidad de tener conocimientos técnicos específicos. Esto es especialmente importante en entornos remotos y distribuidos, como las plataformas petrolíferas en alta mar, donde el acceso in situ puede resultar complicado, así como en situaciones en las que el tiempo sea crucial, como la reanudación de las operaciones en una línea de producción. También existe la posibilidad de llevar a cabo la recuperación con un reinicio a partir de una copia de seguridad del disco local o desde la nube de Acronis. Además, los datos de la copia de seguridad se analizan automáticamente en busca de malware y se actualizan con el último antivirus disponible.

Toda la información y las opciones de control se agregan en un panel de control centralizado denominado Acronis Centralized Monitoring Hub, que utiliza metadatos tanto para realizar análisis como para la integración con software de terceros.

Información de la empresa

Antecedentes

Fundada en Singapur en 2003 y establecida en Suiza en 2008, hoy Acronis emplea a más de 1800 personas en 45 ubicaciones diferentes. Ofrece sus servicios a más de 750 000 clientes corporativos en 150 países.

Desde que empezó a ofrecer servicios de protección de datos, el proveedor ha experimentado un crecimiento significativo en los últimos años, hasta llegar a ofrecer toda una gama de productos de ciberseguridad a sus partners y clientes. También ha sido una empresa pionera en el concepto de fusionar ambos campos con su plataforma Acronis Cyber Protect.

Acronis hace especial hincapié en la investigación y el desarrollo con Acronis Labs, que cuenta con más de 500 ingenieros, más de 20 con doctorado, y ha obtenido más de 200 patentes en sus 17 años de existencia. La Unidad de investigación de amenazas (TRU) de Acronis también publica periódicamente información útil y nuevos hallazgos sobre ciberamenazas actuales y emergentes.

En agosto de 2024 se anunció que EQT, una empresa europea de capital privado, adquiriría una participación mayoritaria en Acronis por un valor estimado de 4000 millones de dólares. Se espera que esta transacción se complete en el primer o segundo trimestre de 2025. Antes de esto, Acronis había recaudado más de 500 millones de dólares de inversores como CVC Capital Partners, BlackRock y Goldman Sachs.

Posición actual

Acronis dispone de una serie de tecnologías de ciberseguridad que van más allá de la copia de seguridad y la recuperación en el ámbito de la OT, incluido su nuevo producto Detección y respuesta ampliadas (XDR) y su asistente de apoyo basado en inteligencia artificial (IA) generativa. El catálogo del proveedor abarca en términos generales lo siguiente:

- Protección de datos (comentada previamente).
- Ciberseguridad (seguridad de endpoints, prevención de malware, EDR/XDR, etc.).
- Administración de endpoints (administración de parches, administración de vulnerabilidades, acceso remoto, etc.).

Aunque parte de la actividad empresarial de Acronis consiste en la venta directa de sus productos a los usuarios finales, su principal vía de comercialización es a través del canal, en el que se incluyen los revendedores, los proveedores de servicios gestionados (MSP) y los fabricantes de equipos originales (OEM). En el ámbito de la automatización industrial, estos incluyen a varios proveedores, como ABB, Emerson, Siemens, Schneider Electric, Rockwell Automation y Yokogawa.

Cabe destacar que Acronis ofrece una versión de servicio básico sin cargo ("freemium") de su plataforma, con la posibilidad de adquirir funciones más avanzadas que se pagan según su uso.

Planes para el futuro

Aunque Acronis tiene previsto desarrollar su plataforma de IA con más funciones de ciberseguridad, de momento no tiene la intención de abordar ámbitos como el de internet de las cosas (IoT) o el de la tecnología operativa (OT).

Datos clave

Tabla 1: Ficha técnica: Acronis

Nombre del producto	Acronis Cyber Protect	Clasificación del producto	Protección de endpoints y copia de seguridad/recuperación
Número de versión	v16	Fecha de lanzamiento	Febrero de 2024
Sectores cubiertos	Fabricación Sanidad Investigación en laboratorio (también conocido como el sector "biofarmacéutico") Petróleo y gas Generación de energía/electricidad Logística Automoción Comercio minorista Educación/administración Construcción	Regiones cubiertas	América del Norte América Central y del Sur EMEA APAC
Tamaño de las empresas objetivo	Grandes empresas y pymes	Opciones de licencia	Licencias de software perpetuas o de suscripción
URL	www.acronis.com https://www.acronis.com/en-us/products/cyber-protect-enterprise/	Vías de comercialización	Venta directa
Sede de la empresa	Schaffhausen, Suiza	Número de empleados	~2000

Fuente: Omdia

Comentario del analista

Las numerosas innovaciones y la especialización de Acronis en el ámbito de la protección y recuperación de datos han dado lugar a una oferta atractiva para entornos industriales. Acronis proporciona varias opciones de despliegue, copia de seguridad y recuperación, lo que no solo ofrece un alto grado de flexibilidad, sino que además permite satisfacer las necesidades específicas de cada cliente. Muchos de los proveedores de seguridad de OT con los que pueden asociarse los proveedores de servicios o los proveedores de automatización industrial no ofrecen funciones de recuperación de datos, lo que supone una gran oportunidad para Acronis. Sus competidores en el ámbito de la recuperación de datos tienden a centrarse más en los entornos de TI. Además, carecen de la especialización que Acronis puede ofrecer en entornos industriales, y no cuentan con la reputación que Acronis ha adquirido gracias a su estrecha integración y a sus alianzas con los principales OEM industriales.

Dicho esto, Acronis ofrece la plataforma más amplia para el canal y sus partners, aunque no cumple los requisitos de seguridad de OT más allá de la "recuperación" y actualmente no tiene previsto hacerlo. Sus partners MSP y proveedores de servicios de seguridad gestionados (MSSP) están más centrados en proporcionar servicios de TI a usuarios finales. Además, para entrar en el ámbito de IoT/OT con una solución de operaciones de seguridad, es probable que se requiera un desarrollo importante, dadas las conductas de los dispositivos y los protocolos patentados. La plataforma permitiría a los partners ofrecer funciones esenciales relacionadas con la seguridad de entornos de TI, pero es probable que recurran a otros proveedores de seguridad de OT para obtener funciones de detección, prevención y visibilidad, con el fin de dar soporte a los clientes industriales en caso necesario. Aunque los líderes en seguridad de OT no se centran actualmente en funciones de protección de datos y recuperación, existe la posibilidad de que estos proveedores también intenten llenar ese vacío, lo que daría lugar a un panorama más competitivo.

Apéndice

On the Radar

"On the Radar" es una serie de notas de investigación sobre proveedores que aportan ideas, productos o modelos de negocio innovadores a sus nichos de mercado. Los proveedores que aparecen en "On the Radar" merecen atención por su posible impacto en el mercado, ya que su enfoque, sus recientes desarrollos o su estrategia podrían resultar disruptivos e interesantes para los compradores y usuarios de tecnología.

Lectura adicional

[*Omdia Market Radar: OT Cybersecurity Platforms, 2025*](#) (enero de 2025)

[*2025 Trends to Watch: IoT Cybersecurity*](#) (septiembre de 2024)

[*"Xage Security announces new partnership with Armis and Yokogawa Engineering Asia to provide secure remote access"*](#) (septiembre de 2024)

[*Omdia Secure Industrial Networks Survey 2023: Overall Findings*](#) (diciembre de 2023)

Autor/a

Hollie Hennessy, analista principal, ciberseguridad de IoT

askananalyst@omdia.com

Política de citas

Solicite la citación y el uso externos de la investigación y los datos de Omdia a través de citations@omdia.com.

Consultoría de Omdia

Esperamos que este análisis le ayude a tomar decisiones empresariales bien fundamentadas y creativas. Si necesita algo más, el equipo de consultoría de Omdia puede ayudarle. Para obtener más información sobre la consultoría de Omdia, póngase en contacto con nosotros directamente en consulting@omdia.com.

Aviso sobre los derechos de autor y descargo de responsabilidad

La investigación, los datos y la información de Omdia a los que se hace referencia en el presente documento (en adelante, los "Materiales de Omdia") son propiedad con derechos de autor de TechTarget, Inc. y sus filiales o afiliados (en conjunto, "Informa TechTarget") o de sus proveedores de datos de terceros, y representan datos, investigaciones, opiniones o puntos de vista publicados por Informa TechTarget, y no constituyen afirmaciones de hechos.

Los Materiales de Omdia reflejan información y opiniones de la fecha de publicación original y no de la fecha de este documento. La información y opiniones expresadas en los Materiales de Omdia están sujetas a cambios sin previo aviso, por lo que Informa TechTarget no tiene la obligación ni la responsabilidad de actualizar los Materiales de Omdia ni esta publicación.

Los Materiales de Omdia se proporcionan "tal cual" y "según disponibilidad". No se ofrece ninguna representación o garantía, expresa o implícita, en cuanto a la imparcialidad, exactitud, integridad o corrección de la información, opiniones y conclusiones contenidas en los Materiales de Omdia.

En la medida máxima permitida por la ley, Informa TechTarget y sus filiales, gerentes, directores, empleados, agentes y proveedores de datos externos declinan toda responsabilidad (incluida, entre otras, cualquier responsabilidad derivada de un acto ilícito o negligencia) en cuanto a la exactitud, integridad o el uso de los Materiales de Omdia. Informa TechTarget no será bajo ningún concepto responsable de las decisiones comerciales, de negociación, inversión o de otro tipo que se basen en los Materiales de Omdia o se tomen en función de los mismos.

CONTÁCTENOS

omdia.com

askananalyst@omdia.com