

MEJORA RÁPIDA DE LAS OPERACIONES DE TI, LA ASISTENCIA Y LA PRODUCTIVIDAD DE LOS EQUIPOS DE LOS MSP

Libro electrónico encargado
por **Acronis**



ÍNDICE

Mejora rápida de las operaciones de TI, la asistencia y la productividad de los equipos de los MSP 3

Las API, amadas y odiadas por igual..... 4

El verdadero coste de la fragmentación de las herramientas 5

Bienvenidos a la solución bien integrada..... 6

La importancia de la madurez de las empresas..... 8

Sobre la importancia de invertir en la pila completa..... 9

Conclusión..... 10

Referencias..... 11

Recursos adicionales 12



MEJORA RÁPIDA DE LAS OPERACIONES DE TI, LA ASISTENCIA Y LA PRODUCTIVIDAD DE LOS EQUIPOS DE LOS MSP

Karl W. Palachuk

En diciembre de 2019, Boeing lanzó su nave espacial Starliner en una misión que la llevaría hasta la Estación Espacial Internacional. La misión era simple: lanzamiento, acoplamiento con la Estación Espacial Internacional y regreso sin daños a la Tierra.

Cincuenta y cinco minutos después del lanzamiento, la NASA informó de que la Starliner experimentó una "inserción orbital no nominal". Es la jerga técnica para decir que la nave estaba en la órbita equivocada.

Y no llegó a la Estación Espacial Internacional. ¡Se había desviado! Por suerte, se trataba de un vuelo de prueba no tripulado.

En un mundo de precisión absoluta, ¿cómo pudo suceder este fallo? Dicho de forma sencilla, dos sistemas de software diferentes no consiguieron comunicarse a la perfección entre sí. Aunque se pusieron todos los medios para que hubiera una comunicación abierta e impecable, se pasó por alto un pequeño detalle técnico: el reloj de a bordo no tenía la hora correcta, por lo que la nave no estaba donde debía cuando debía.

Parémonos a pensarlo un momento: la NASA, SpaceX y Boeing se comprometen a trabajar juntas en un entorno de cooperación franca. Los tres socios comparten entusiasmo y objetivos. Todos reman en la misma dirección en pos del mismo resultado.

La inversión total de Boeing fue de 1500 millones de dólares para que nada fallara. Pero falló.

Esto puede enseñarnos una lección importante sobre la relación entre complejidad, interconexiones y eficacia a la hora de utilizar aplicaciones de software. Incluso trabajando sobre la base de especificaciones de diseño acordadas y de plataformas totalmente abiertas y bien documentadas, las cosas pueden salir mal.

Ahora imaginemos un entorno en el que los desarrolladores no sean socios, sino competidores. Cada uno publica los requisitos para conectarse a través de su interfaz de programación de aplicaciones (API), pero no se comunican directamente entre sí.

El resultado es el que cabría esperar: más complicaciones, menos agilidad y mayor propensión a problemas.

LAS API, AMADAS Y ODIADAS POR IGUAL

La tecnología siempre se mueve rápido. Mientras en otros sectores hay que esperar diez años para que surja un nuevo negocio, en el mundo de las TI nace una nueva generación de tecnologías cada 18 o 24 meses. Si su manera de desempeñar su actividad no ha cambiado en cinco años, sin duda se ha quedado desfasado.

Al adentrarnos en 2021, nos encontramos en una era dominada por las API, que surgieron a principios de siglo como forma de ayudar a que las aplicaciones trabajaran juntas, intercambiaran información y automatizaran procesos.

Las API fueron un compañero perfecto para muchos proveedores de servicios gestionados, pues permitían que herramientas diferentes funcionasen juntas. Por supuesto, cuanto más middleware de API se comprasen, mayor era el coste de la prestación de los servicios. A veces, ese middleware era bastante caro y, con demasiada frecuencia, un tanto chapucero, ¡pero cumplía!

Lo que en un momento dado fue una nueva y maravillosa estrategia se había convertido en un kit de "construcción de un monstruo de Frankenstein informático".



Ya en el presente, las API han madurado mucho. Pero, incluso en las circunstancias más favorables y con la mejor programación, sigue haciendo falta gestionar las conexiones entre API. Cuando se conectan programas de dos empresas distintas, un cambio en cualquiera de ellos puede "romper" funciones. Si para colmo la conexión entre los dos es de un tercero, se complica todavía más.

Toda conexión requiere un mínimo de administración y, al mismo tiempo, representa un posible agujero de seguridad que hay que vigilar. El ransomware se ha convertido en un gran negocio y los ciberdelincuentes han descubierto en los proveedores de servicios de TI objetivos propicios para robar datos y propagar código. Pueden escoger un punto de entrada cualquiera para sus ataques y percutir contra él, por lo que hay que defenderlo todo.

El secreto inconfesable de todo desarrollo de software es que el mantenimiento y el soporte siempre acaban costando más que el software en sí. (Como proveedores de servicios de TI, lo sabemos porque vivimos prestando una parte de ese soporte). Además, cada grupo de conexiones aumenta la necesidad de supervisión, mantenimiento y soporte.

EL VERDADERO COSTE DE LA FRAGMENTACIÓN DE LAS HERRAMIENTAS

Por si no bastara con pagar a varios proveedores de software, la "fragmentación de las herramientas" implica mayores costes de formación, integración y mantenimiento. Un estudio de Gartner señaló que esa complejidad provoca el aumento de los gastos en varios frentes. Al final, lo "odiado" de las API radica en el hecho de que, si bien conectan varias aplicaciones de software, lo hacen con poca eficacia. Cada conexión añade complejidad, documentación, formación y dos o más conexiones adicionales y su mantenimiento correspondiente.

El esfuerzo que implica mantener un sistema complejo e interconectado también incide directamente en la productividad general. Cada hora dedicada al mantenimiento de los sistemas propios es una hora en la que no se ayuda a los usuarios.

En un estudio reciente, Forrester Research constató que el uso de herramientas tradicionales suponía un importante obstáculo para la modernización y la transformación digital. Un 86 % de las empresas usan al menos una herramienta antigua, y solo un 12 % usan únicamente herramientas de supervisión modernas y totalmente integradas.

Esta dependencia de herramientas obsoletas y mal conectadas se traduce en costes más altos para el soporte del entorno, en la degradación de la prestación del servicio y en mayores riesgos para la seguridad (volveremos a esto más adelante). Otro coste frustrante del uso de un gran número de herramientas es la integración. Casi la mitad (46 %) de las empresas informaron de que "les cuesta demasiado tiempo y dinero mantener e integrar los diferentes protocolos de seguridad de cada herramienta".

Además de todo eso, se produce solapamiento entre las funciones de las herramientas. Dicho de otro modo, pagas por lo mismo dos o tres veces. En cada caso, al menos una de las herramientas deja de usar todas las funciones que integra, porque se usa una función parecida de otro software. Este solapamiento implica que casi todas las herramientas están infrautilizadas por la complejidad, la falta de recursos o la carga que implica gestionarlas.

En resumen, la mayoría de las empresas usan varias herramientas que no están diseñadas para su conexión. Gastan en herramientas con funciones duplicadas, lo que aumenta los costes de mantenimiento y la inversión inicial en licencias. Su funcionamiento requiere más formación, más supervisión y más documentación con cada producto que se añade al conjunto.

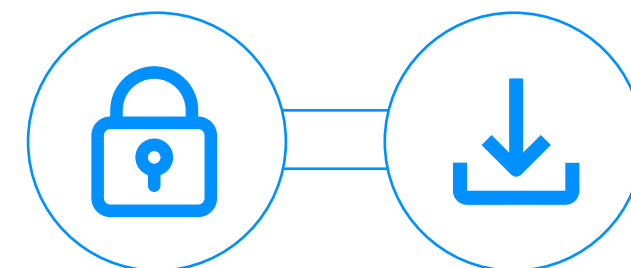
BIENVENIDOS A LA SOLUCIÓN BIEN INTEGRADA

Hemos avanzado mucho desde las toscas API iniciales. Cada vez más, los equipos de TI eligen opciones de software que se diseñan para integrarse, en lugar de parchearse después. Dejamos atrás el mundo dominado por la traducción de las API.

La complejidad es un factor importante en el desarrollo y mantenimiento de software. No es de extrañar que la complejidad aumente el gasto en mano de obra para mantenimiento, seguridad y soporte.

Ejemplo 1

Con dos soluciones de software y un conector, es posible que hasta tres proveedores deban trabajar juntos. Cualquiera de ellos puede hacer algún cambio que interrumpa la conexión o genere una vulnerabilidad susceptible de ser aprovechada.



Ejemplo 2

Con tres soluciones de software y dos conectores, es posible que hasta cinco proveedores deban trabajar juntos. De nuevo, cualquiera de ellos puede hacer un cambio que corte la conexión o genere una vulnerabilidad.



Ejemplo 3

Analicemos ahora el incipiente mundo "integrado" de las aplicaciones de seguridad. Se trata de aplicaciones diseñadas para funcionar juntas desde el principio. Las crea el mismo equipo. Están diseñadas para funcionar juntas.



Cuando se tienen sistemas distintos para copia de seguridad, protección contra malware, escritorio remoto y administración, también hay multitud de conexiones, y cada una representa varias fuentes posibles de problemas y vectores de amenaza dentro de ese entorno. A continuación paso a explicar lo que quiero decir.

Supongamos que desea conectar dos aplicaciones y sus servicios, como copia de seguridad y antivirus. En la práctica, esta situación puede darse con diferentes variantes. ¿Están desarrolladas ambas por la misma empresa? ¿Están diseñadas para trabajar juntas desde el principio? Si hay una conexión entre los dos sistemas, ¿es obra de una de esas empresas o de un tercero?

Reduciendo la complejidad del software, disfruta de las ventajas de una mayor eficiencia, productividad y seguridad y de un menor mantenimiento. También disminuye los costes desde el primer momento, pues no paga por un middleware de terceros para que funcione la pila de aplicaciones ni por el tiempo adicional que hay que dedicar a gestionar más aplicaciones.

Entre los proveedores de servicios de TI existe un problema creciente: demasiadas facturas de demasiadas empresas por hacer que los sistemas funcionen correctamente.

Hay una empresa que ha hecho frente a este problema sin rodeos. Acronis ha desarrollado una pila de productos que trabajan sin problemas entre sí. Basada en la integración completa de sus distintos componentes, la solución Acronis Cyber Protect maximiza la eficacia gracias a que reduce la complejidad y el coste total de propiedad. En palabras de Lauren Beliveau, directora de marketing de productos de Acronis, "no tenemos un montón de productos, tenemos una pila de soluciones".

No se trata de un mero problema teórico. En el mundo de la seguridad, la clásica "amalgama" de herramientas antiguas supone una amenaza grave que exige un mayor esfuerzo de

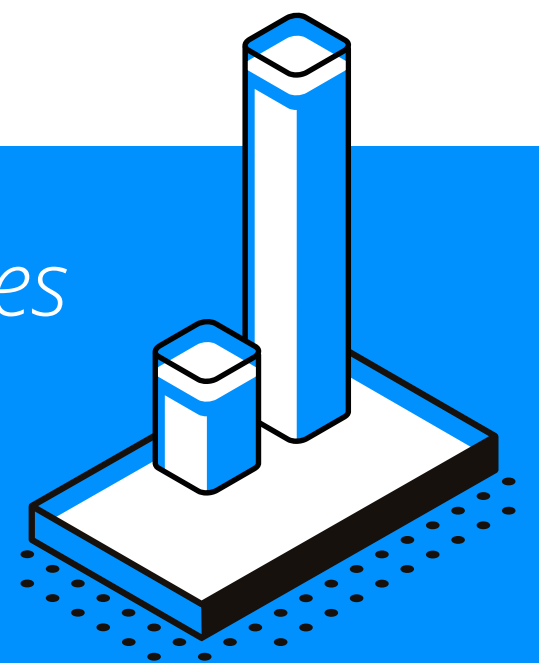
supervisión. Cada conexión representa una posible vulnerabilidad, pero lo mismo ocurre con cada parche o actualización. No solo hay que aplicar parches, también se debe vigilar todo para cerciorarse de que no han creado un problema. A veces, se deben quitar los parches o poner otros conforme surgen vulnerabilidades.

Por desgracia, un método habitual de la aplicación de parches es esperar cierto tiempo antes de aplicarlos para estar seguro de que no crean nuevos problemas, incompatibilidades o deficiencias. Esta práctica prolonga la exposición de las aplicaciones a vulnerabilidades conocidas.

Por si fuera poco, puede que aplicaciones mal integradas de diferentes proveedores no compartan datos, alertas, automatizaciones, documentación, interfaces de usuario o agentes, etc. Cada punto débil de una conexión constituye un riesgo para la seguridad. Hoy día, el coste de estas deficiencias es demasiado grande para pasarlo por alto.

Con Acronis Cyber Protect, el antivirus sabe que hay una copia de seguridad y la analiza. Al ser una solución totalmente integrada, se consigue un mejor funcionamiento conjunto de herramientas como la copia de seguridad y el antivirus. Las copias de seguridad se analizan automáticamente para asegurar que no contengan amenazas, como virus, malware o ransomware. Los parches se aplican a las copias de seguridad y también a los sistemas activos. Todo ello sin costuras. Literalmente.

A menor complejidad del software, mayor es la eficacia, la productividad y la seguridad, y menor el mantenimiento



LA IMPORTANCIA DE LA MADUREZ DE LAS EMPRESAS

Otro factor que raramente se tiene en cuenta es la madurez de las empresas que fabrican las herramientas. Por lo general, desde que son meras startups hasta que alcanzan la madurez completa, las empresas atraviesan varias fases. Al principio, tienen un producto inmaduro con una única funcionalidad (por ejemplo, un antivirus). Con el tiempo, el producto llega a ser totalmente funcional. En su evolución, las empresas se centran en comercializar el producto y puede que incluso en ganar dinero.

Conforme se consolidan, buscan aumentar las funciones y la conectividad, por lo que adoptan las todopoderosas API. Su objetivo en esta etapa es conectarse con todo el mundo. Tal vez sea cuando más parches se improvisen. Funciona, la mayor parte del tiempo, pero las API no son maduras y todo cambia continuamente. Si son eficaces, los usuarios demandan más y más funciones, por lo que avanzan a la siguiente etapa: ampliar su base de usuarios.

Las empresas centradas en esta ampliación también se preocupan por adquirir o crear nuevas funciones. Su estrategia a estas alturas es captar clientes ofreciendo más funciones

y colaborando con más competidores. El objetivo último es conseguir cuota de mercado respondiendo a las demandas de los usuarios y haciendo más con sus herramientas. La fase de expansión también es un momento de grandes cambios internos y de intentar adaptarse a API que evolucionan constantemente, a nivel interno, entre los productos que compran e integran, y también entre sus productos y sus competidores.

La siguiente etapa es la expansión financiera. Ya sea mediante capital riesgo o con alguna otra fuente de financiación, llega un momento en que las empresas necesitan dinero para crecer. Eso, a su vez, hace que baje la capacidad de respuesta ante los clientes. La atención de los directivos se desvía progresivamente de la funcionalidad a la financiación, y es más importante vender que solucionar problemas o añadir funciones.

Este fenómeno se observa en las fusiones a lo largo de los años: un proveedor que siempre respondía deja repentinamente de solucionar problemas y la hoja de ruta del producto se vuelve un misterio para los profesionales de TI que usan el software. En esta fase, las ventas acaparan toda la actividad de la empresa. El desarrollo (incluso la corrección de errores) se reduce de manera considerable.

Solo un puñado de empresas viven lo suficiente para madurar de verdad, desarrollando herramientas bien integradas que funcionan juntas sin problemas, y con suficiente soporte

a nivel de programación para añadir nuevas funciones sin alterar nada ni crear nuevos problemas. Además de los retos técnicos, las empresas maduras han establecido un patrón a largo plazo de financiación de desarrollo constante, además de ventas y atención al cliente.

Como la tecnología cambia más rápido cada año, se necesitan funciones nuevas para afrontar los retos que surgen. Este hecho se observa en la ciberseguridad más que en ningún otro sector. Hace diez años, los virus eran molestos y destructivos. En la actualidad, amenazas como el ransomware pueden costar millones de dólares, que se suman al coste provocado por el tiempo de inactividad.

Las empresas menos maduras y las que se han desviado por fusiones y adquisiciones tienen que aguantar con productos más antiguos. Con demasiada frecuencia, no disponen de tiempo, fondos o capacidad para afrontar las exigencias de un entorno de seguridad que evoluciona sin cesar.

En el mejor de los casos, cuentan con soluciones antiguas. En el peor, sus soluciones no se integran con las herramientas más modernas.

La complejidad del conjunto de herramientas es inversamente proporcional a la eficiencia. Además, para resolver el problema del uso de múltiples API, debe gestionar la actividad interna del software con diferentes grados de madurez, el soporte de empresas con diferentes niveles de madurez en sus API, y la documentación.

En esta situación, su objetivo es construir una pila eficaz. En ocasiones esto implica buscar las mejores opciones del mercado, aunque sean de proveedores distintos. Siempre que sea posible, conviene comprometerse mucho con una sola pila para así aumentar la eficacia, la seguridad y el beneficio.

Con Acronis Cyber Protect, ahora lo tiene todo. Acronis cuenta con el reconocimiento general como líder en protección y recuperación de datos. Ha creado todo un conjunto de soluciones de primera clase para proteger datos, aplicaciones y sistemas, y eliminar el problemático "software intermediario", el middleware.

Acronis Cyber Protect incluye funciones que la competencia se apresurará a copiar, incluida la aplicación de parches a las imágenes de copia de seguridad para que los procedimientos de restauración no devuelvan a un nivel de seguridad inferior las máquinas cliente.

Ante este panorama de ransomware, demandas multimillonarias y normativas oficiales, la década que inauguró 2020 no es momento de perder dinero y trabajo armando una colección de herramientas de seguridad con la esperanza de que funcionen bien juntas. Se necesitan soluciones que tengan lo último en funcionalidad y seguridad y, al mismo tiempo, reduzcan la complejidad, el mantenimiento y los costes que conllevan.

Pásese a la única pila de seguridad diseñada desde el principio para estar totalmente integrada.



CONCLUSIÓN

"En Acronis Cyber Protect tenemos realmente una solución capaz de hacer por sí sola el trabajo de diez soluciones por separado".

Jason Menezes,

jefe del departamento de copia de seguridad y recuperación ante desastres de Datategra

La seguridad ya no puede considerarse una función que simplemente se añada a otros servicios. En la actualidad, los consultores de tecnología tienen que disponer de soluciones completas y sólidas que ofrezcan una seguridad incomparable sin importunar a los usuarios.

La complejidad disminuye la eficiencia y la productividad, al tiempo que aumenta los costes de mantenimiento, documentación y formación. Cuantas más "piezas" haya, más conectores se necesitarán. Una pila totalmente integrada, diseñada para funcionar sin fisuras, maximiza la seguridad general y disminuye la complejidad y todos los costes que implica.

Las API seguirán con nosotros mucho tiempo. Por suerte, después de hacer la transición a la pila totalmente integrada de Acronis, el líder en ciberseguridad y protección de datos, es posible ser productivo administrando sistemas complejos interconectados.

Las conexiones están bien. La integración por diseño está mejor.

REFERENCIAS

<https://www.msn.com/en-us/news/technology/boeings-software-troubles-show-an-engineering-culture-clash/ar-BB16xEdq>

<https://www.forbes.com/sites/jonathanocallaghan/2019/12/20/boeing-starliner-spacecraft-launches-to-the-international-space-station-heralding-a-new-era-for-american-human-spaceflight/>

If This Then That

<https://ifttt.com/>

Zapier

<https://zapier.com/>

Programmable Web

<https://www.programmableweb.com/>

Salesforce.com

www.salesforce.com

Harvard Business Review, "The Strategic Value of APIs" (El valor estratégico de las API)

<https://hbr.org/2015/01/the-strategic-value-of-apis>

"Gartner afirma que las empresas pueden recortar un 30 % en costes de software con tan solo utilizar tres mejores prácticas".

<https://www.gartner.com/en/newsroom/press-releases/2016-07-19-gartner-says-organizations-can-cut-software-costs-by-30-percent-using-three-best-practices>

Forrester Research, "Prevalence Of Legacy Tools Paralyzes Enterprises' Ability To Innovate" (La prevalencia de las herramientas tradicionales paraliza la capacidad de innovación de las grandes empresas).

<https://sciencelogic.com/wp-content/uploads/sciencelogic-os.pdf>

"Struggling With Toolchain Sprawl? You're Not Alone" (¿Problemas con la fragmentación de la cadena de herramientas? No es el único).

<https://dzone.com/articles/toolchain-sprawl-youre-not-alone>

ACERCA DEL AUTOR



Karl W. Palachuk ha creado y vendido dos empresas de servicios gestionados en Sacramento (California). Es el fundador y presidente del Sacramento SMB IT Professionals Group. Ha escrito varios libros, entre otros *The Network Documentation Workbook* y *Managed Services in a Month*.

Desde hace más de 15 años, interviene como ponente destacado en congresos y seminarios de todo el mundo. Es ingeniero de sistemas certificado por Microsoft, además de poseer un grado por la Universidad Gonzaga y un máster por la Universidad de Michigan. También es Microsoft Small Business Specialist y miembro del Microsoft's Small Business Specialist Advisory Panel desde su creación.

RECURSOS ADICIONALES

CASE STUDY

HomeBuys Looks to Do More with Less with Acronis Cyber Protect 15

Retail upstart able to consolidate multiple IT tools for backup, antimalware, remote desktop, and patch management into a single console.

INTRO

HomeBuys is a discount retailer established in 2015 with six locations in Ohio and one in Kentucky. Its founders, who have decades of experience in retail – most notably with the Big Lots brand – wanted to offer an uncommon experience to customers. To do so, HomeBuys utilizes closeout buying opportunities from major big box retailers and other sources, thereby passing the savings onto its customers on high quality items from food to wine to home décor. With a constantly changing inventory, the retailer lives by its tagline: “The Best for Less.”

CURRENT IT ENVIRONMENT AND SECURITY SOLUTIONS USED

HomeBuys’ IT environment encompasses its six stores, one distribution center, and its corporate office. Not surprisingly for a retailer, the most mission-critical application infrastructure is its ERP system, NetSuite, which was migrated to relatively recently from Microsoft Dynamics. In terms of data protection, the company uses Unitrends for bare metal backup and restore and an appliance from iDrive for backup and restore of virtual environments. For endpoint protection of workstations and laptops, HomeBuys uses a combination of LogMeIn and Windows Defender, while some servers use McAfee.

In total, HomeBuys’ network administrator Jorge Alexandres is responsible for protecting more than 1.5TB of historical data. The retailer does not currently use Acronis. Acronis Cyber Backup had been previously evaluated but at the time it did not have the right functionality and integration for Microsoft Dynamics.

Then Alexandres received an invitation to participate in the beta program of Acronis Cyber Protect 15. The product’s value proposition interested him, so he joined the beta.

BETA IMPRESSIONS

- Easy to install and use
- Powerful, multi-purpose tool

PROTECTED RESOURCES

- 1.5TB
- 30 workstations
- 4 servers

OPPORTUNITY AHEAD

- Consolidate three separate IT tools
- Gain operational and financial efficiencies



www.acronis.com

Copyright © 2002-2020 Acronis International GmbH.

Blog de Acronis: ofrece las últimas novedades y análisis del líder mundial en ciberprotección.

Canal de Acronis en YouTube: presenta vídeos de casos de uso, demostraciones, análisis de ciberamenazas y noticias de la empresa.

Centro de recursos de Acronis: reúne documentos técnicos, libros electrónicos, artículos especializados, tutoriales, infografías, etc., sobre ciberprotección.

Eventos de Acronis: aquí se publican eventos, seminarios web, entrevistas, etc., con información para inscribirse.

ACERCA DE ACRONIS

Acronis unifica protección de datos y ciberseguridad para ofrecer una [ciberprotección](#) integrada y automatizada que resuelve los retos de salvaguarda, accesibilidad, privacidad, autenticidad y seguridad ([SAPAS](#)) en el mundo digital moderno. Con modelos de implementación flexibles que se adaptan a las necesidades de los proveedores de servicios y los profesionales de TI, Acronis proporciona una ciberprotección de primera línea para datos, aplicaciones y sistemas, con soluciones innovadoras de [antivirus de próxima generación](#), [copia de seguridad](#), [recuperación ante desastres](#) y [administración de la protección de endpoints](#). Gracias a sus galardonadas tecnologías [antimalware con inteligencia artificial](#) y de [autenticación de datos basada en blockchain](#), Acronis protege cualquier entorno, [en la nube, híbrido o local](#), por un precio reducido y previsible.

[Fundada en Singapur](#) en 2003 y establecida en Suiza en 2008, hoy Acronis emplea a más de 1500 personas en 33 ciudades de 18 países. Sus soluciones cuentan con la confianza de más de 5,5 millones de usuarios particulares y 500 000 empresas, incluidas el 100 % del Fortune 1000, y equipos deportivos profesionales de primer nivel. Los productos de Acronis están disponibles en más de 40 idiomas a través de 50 000 partners y proveedores de servicios de más de 150 países.

Libro electrónico encargado por **Acronis**

acronis.com

