Acronis

El ransomware en 2023:

Información sobre el mercado y protección transversal del NIST con Acronis

Presentación de las tendencias de ransomware para 2023 y por qué Acronis obtuvo la Medalla de Oro en el cuadrante de datos, categoría de protección de endpoints, en SoftwareReviews 2022

INFO~TECH
RESEARCH GROUP

SoftwareReviews

Índice

Tendencias del ransomware: una amenaza en constante evolución

En 2022, más del 30 % de las organizaciones de todo el mundo sufrieron un ataque de ransomware y, como resultado, se les negó a los empleados el acceso a sus archivos y las empresas perdieron millones de dólares en pagos extorsivos. RiskRecon analizó 633 eventos de ransomware publicados entre 2017 y 2021 que interrumpieron las operaciones con técnicas de cifrado. Este año, no hay señales de que los ataques de ransomware vayan a reducirse, en tanto que los ciberdelincuentes continúan apuntando a organizaciones de todo tipo y tamaño, siguen surgiendo distintas variantes de malware existente y constantemente aparecen otras nuevas.

Para asegurarnos de que su organización siga siendo #CyberFit y resiliente frente a un ataque de ransomware, nos reunimos con Carlos Rivera, director asesor principal de Info-Tech Research Group, para conocer su opinión sobre las tendencias y sobre cómo protegernos de las ciberamenazas.

1 Según su investigación, ¿cuáles son las principales tendencias en ransomware que las organizaciones deberían tener en cuenta en 2023?

Carlos Rivera

Asesor principal de Investigación en Seguridad y Privacidad
Info-Tech Research Group

En mi opinión, la mayor tendencia que observaremos en 2023 es un aumento de los intermediarios de acceso inicial (IAB).

Los IAB siguen un modelo de contratación similar al ransomware como servicio. Adquieren a un grupo de ciberdelincuentes el acceso a una red corporativa afectada y, después, otorgan a un agresor el punto de partida para preparar su ataque.

Otra tendencia que observamos es el ransomware como servicio (RaaS). Algunos ciberdelincuentes ahora ofrecen RaaS y, con ello, favorecen enormemente la preparación de un ataque a nivel global. Proporcionan las herramientas y la infraestructura para que otros perpetren ataques de ransomware a cambio de una tajada del rescate. El año 2022 también fue testigo del regreso de Lockbit 3.0, una nueva versión de la conocida plataforma de ransomware como servicio que ostenta el récord por tener la tasa de cifrado más rápida del mercado.

Tendencias del ransomware

Por último, las organizaciones deben estar alertas respecto de la doble extorsión. Se trata de una combinación de ataques de ransomware y extorsión. En el ataque, el delincuente despliega malware con el que logra cifrar los datos y filtrarlos. Extrae los datos confidenciales antes de cifrar los archivos y desplegar sus pedidos de rescate, lo que hace que sea difícil retirarse de las negociaciones. Los delincuentes no solo dejan los datos de la víctima cifrados, sino que comienzan a filtrar información confidencial, algo que provoca importantes daños para la compañía y sus clientes.

Se espera que el ransomware siga siendo una amenaza persistente en 2023, ya que los nuevos carteles se concentran en organizaciones pequeñas y medianas, así como en objetivos poco atractivos con menos probabilidades de llamar la atención de los agentes de cumplimiento de la ley. Esta tendencia también implica un aumento del riesgo para los sistemas de gobierno municipales y comarcales.

> 2 La protección de endpoints hace referencia a las medidas que se adoptan para proteger los dispositivos conectados a la red de una organización, como computadoras de escritorio, computadoras portátiles y dispositivos móviles conectados en red. ¿Por qué a las organizaciones les resulta difícil proteger sus endpoints contra los ataques de ransomware?

Hay muchas complicaciones en juego. En primer lugar, la falta de visibilidad en las redes complejas. Puede ser difícil supervisar la actividad de los endpoints de cada uno de los empleados, lo que dificulta aún más realizar un seguimiento y proteger todos los dispositivos.

Además, la protección de endpoints puede ser particularmente complicada cuando son dispositivos móviles, que a menudo se usan fuera de la red de la organización y no tienen el mismo nivel de seguridad que las computadoras de escritorio.

También está el factor del error humano. Los endpoints suelen utilizarlos empleados que pueden cometer errores perjudiciales para la seguridad, como caer en la trampa de un ataque de phishing o descargar malware.

"Es fundamental tomar medidas para proteger su organización contra los ataques de ransomware. Esto significa mantener el software actualizado, usar contraseñas seguras y autenticación de dos factores, y ser precavido al abrir correos electrónicos o descargar adjuntos y ejecutarlos", recomienda Rivera.

Tendencias del ransomware

3 ¿Cómo pueden prepararse las organizaciones para estas nuevas amenazas?

Muchas organizaciones carecen de la capacidad para organizar un plan efectivo de respuesta ante incidentes. Las guías tácticas de respuesta ante incidentes indican a las organizaciones los pasos para responder ante distintas situaciones, como amenazas de día cero, y también los procedimientos para remitir las posibles violaciones de seguridad a un superior. Quizá algunas empresas no tienen implementados procedimientos de protección de endpoints o respuesta adecuados. Esto puede causar daño al negocio, ya que, si no se implementa la protección de endpoints adecuada, el equipo de seguridad no tendrá conocimiento de un posible ataque de ransomware.

Para abordar estos desafíos, se recomienda a las organizaciones implementar una solución completa e integrada de protección de endpoints. Contar con una solución integrada presenta una gran cantidad de beneficios, ya que equipa a las empresas con una estrategia de ciberseguridad proactiva que permite detectar amenazas externas y reaccionar ante ellas. Con una solución integrada, las empresas también pueden proteger sus datos y colmar insuficiencias, como la falta de un equipo con experiencia en ciberseguridad o el tiempo y los recursos necesarios para gestionar soluciones de ciberseguridad múltiples y complejas.

Además de implementar la solución integrada correcta, las empresas pueden identificar agentes para realizar copias de seguridad regulares de los endpoints críticos de manera tal de satisfacer las expectativas de continuidad de la actividad en un posible evento de ransomware. Los equipos de las organizaciones pueden coordinar las iniciativas y las directivas de seguridad para proteger los datos contra robos o violaciones. A fin de proteger aún más los activos de la empresa, los responsables de seguridad pueden ofrecer cursos de formación internos para capacitar a los empleados sobre las tendencias más recientes en ciberseguridad, las formas de identificar una amenaza y las vías para evitar un ataque de ransomware.

4 ¿Por qué los MSP deberían aprovechar la oportunidad de abordar este problema para las empresas?

En julio de 2022, BlackHat USA encuestó a cientos de asistentes y concluyó que los profesionales de la ciberseguridad están mentalmente exhaustos; en este sentido, poco menos de la mitad manifestó padecer algún tipo de agotamiento mental y disponer de poco tiempo para responder a las amenazas. En esta misma encuesta, más del 60 % afirmó que el mayor reto de la organización estaba en detectar ataques y amenazas en un entorno de TI descentralizado y, tal vez, orientado a la nube. La encuesta también señala que, según el 52 % de los profesionales, la detección de posibles vulnerabilidades en la seguridad de un entorno de TI complejo y descentralizado representa el máximo riesgo de sufrir ciberataques.

Tendencias del ransomware

Los MSP tienen una oportunidad única de ayudar a las empresas a reducir costos e incrementar su eficiencia con servicios de seguridad sólidos y visibilidad de posibles amenazas.

A la larga, los MSP pueden ayudar a sus clientes a proteger su información por medio de soluciones competitivas de recuperación de datos y protección de endpoints. Al permitir que las empresas alcancen el éxito en el entorno digital actual con gastos operativos reducidos, los MSP impulsan su propio crecimiento y se aseguran asociaciones empresariales a largo plazo.

5 ¿Qué es un enfoque transversal del NIST y por qué es importante para mantener un entorno seguro?

Por "enfoque transversal del NIST", se hace referencia a un método de ciberseguridad que implica el uso de múltiples estándares y directrices del National Institute of Standards and Technology (NIST). El NIST es un organismo no regulatorio del Departamento de Comercio de los EE. UU. que desarrolla e impulsa estándares, directrices y mejores prácticas para la tecnología de la información, incluida la ciberseguridad.

El marco de ciberseguridad (CSF) del NIST es un marco de uso generalizado que ofrece orientación para que las organizaciones sepan cómo afrontar y reducir los riesgos de ciberseguridad. Se basa en cinco funciones clave: identificar, proteger, detectar, responder y recuperar. Un enfoque transversal del NIST implica usar múltiples estándares y directrices establecidos por el NIST de manera integrada y coordinada con el objetivo de satisfacer las necesidades de ciberseguridad de la organización. Esto puede significar el uso de múltiples marcos del NIST, como el CSF, y otros estándares y directrices del NIST.

El enfoque transversal del NIST es importante porque permite que las organizaciones protejan sus datos y reduzcan los riesgos para la ciberseguridad. Al adoptar este enfoque, las organizaciones garantizan que sus esfuerzos de ciberseguridad y protección contra el ransomware sean integrales y se ciñan a las mejores prácticas vigentes.

Además, un enfoque transversal del NIST permite que las organizaciones personalicen sus medidas de ciberseguridad en función de sus necesidades al combinar múltiples estándares y directrices del NIST. De este modo, las empresas pueden desarrollar un enfoque de defensa en profundidad que contribuya a prevenir, detectar y responder a los incidentes de ciberseguridad. En última instancia, un enfoque transversal del NIST permite que las organizaciones gestionen y reduzcan sus riesgos de ciberseguridad de manera efectiva, además de tornarse más resistentes ante ciberamenazas tales como los ataques de ransomware.

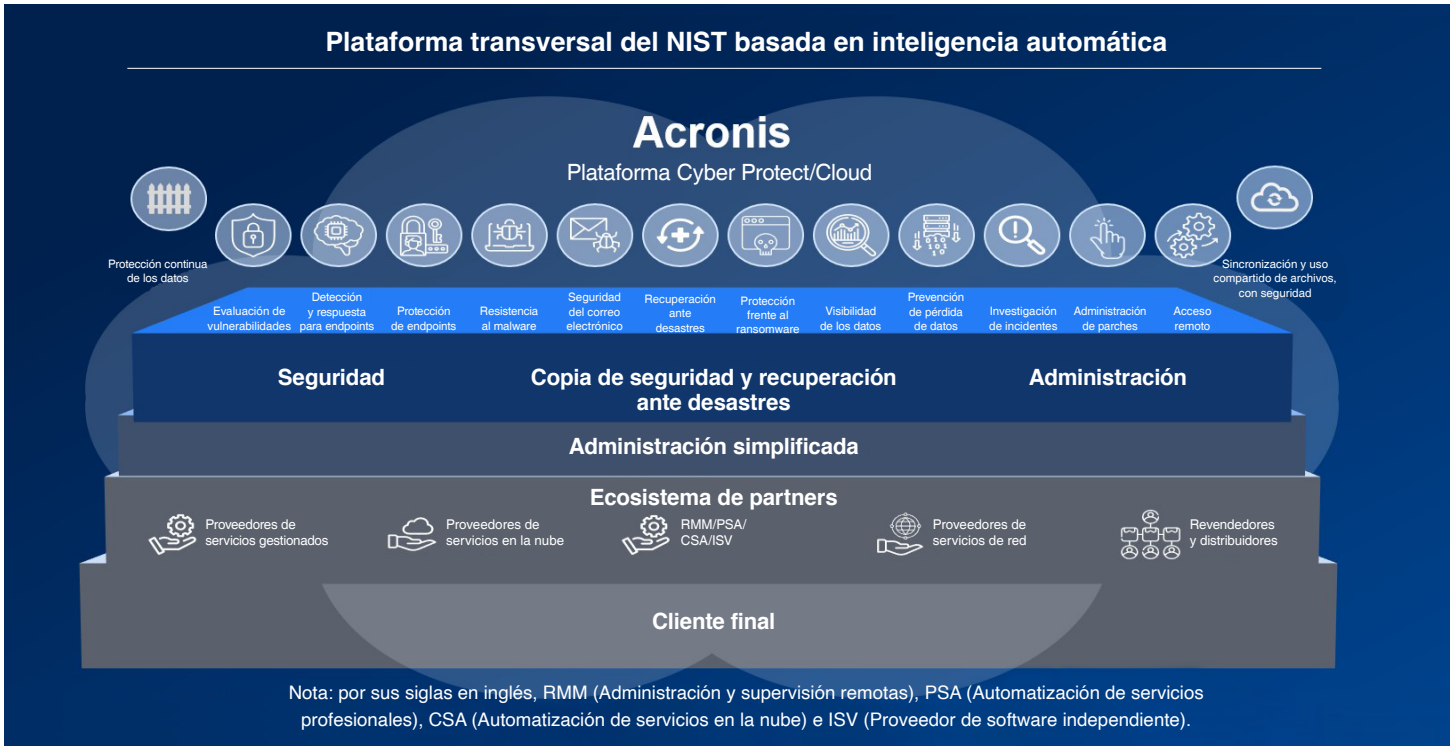
Presentamos la plataforma Acronis Cyber Protect Cloud

Fundada en 2003, Acronis es una empresa proveedora global de tecnología con sede central conjunta en Suiza y Singapur. Su plataforma insignia, Acronis Cyber Protect Cloud, es el producto que utilizan más de 50 000 partners de tecnología (incluidos proveedores de servicios gestionados y distribuidores de valor añadido) en más de 150 países para ofrecer servicios de ciberseguridad, protección de datos y administración de endpoints a más de medio millón de empresas.

La plataforma de Acronis cuenta con el respaldo de Acronis Cyber Cloud, una red global compuesta por más de 50 centros de datos seguros y más de 140 integraciones con proveedores de software independientes. La marca se ve reforzada por Acronis Cyber Protect Home Office, una oferta para particulares con más de cinco millones de usuarios que muchos profesionales de TI citan como el primer producto de copia de seguridad que utilizaron en sus hogares o en la escuela.

Acronis es pionera en ciberprotección (integración de ciberseguridad, protección de datos y administración de endpoints), que los MSP ofrecen como un conjunto de servicios y los VAR como un único producto de software, con un solo agente en cada endpoint y administrado desde una sola consola.

La plataforma de Acronis ofrece un conjunto integral de capacidades para proteger el tiempo de actividad y los datos de las empresas contra ciberataques, fallos de infraestructura, desastres naturales y errores humanos, como se observa en la figura 1:



Funciones de ciberseguridad, protección de datos y administración de endpoints de la plataforma de Acronis

Logre el respaldo del enfoque transversal del NIST con Acronis

Estas funciones incluyen la totalidad del marco de ciberseguridad (CSF) del National Institute of Standards and Technology (NIST) de los EE. UU., un conjunto de estándares y mejores prácticas de uso generalizado para reducir los ciberriesgos. El CSF clasifica las funciones de ciberseguridad en cinco etapas: identificar, proteger, detectar, responder y recuperar. Acronis respalda cada una de estas etapas con una lista amplia y creciente de funciones de protección de datos y ciberseguridad.

Este enfoque integral para proteger el tiempo de actividad y los datos de la empresa ha cobrado vital importancia en un mundo en el que:

- Los ciberdelincuentes generan cientos de miles de iteraciones de malware nuevas todos los días.
- La escala, el ingenio y la capacidad de destrucción de los ataques de ransomware se incrementan año tras año.
- Surgen nuevas herramientas de IA, como ChatGPT, para permitir que los delincuentes poco avezados perpetren ciberataques exitosos basados en el phishing y la explotación de vulnerabilidades conocidas del software.
- Las reglamentaciones de cumplimiento imponen mayores exigencias sobre la manera en que las empresas deben proteger los datos confidenciales y dónde almacenarlos.
- El cambio climático amplía el poder destructor de inundaciones, tormentas e incendios.

Con el respaldo de 500 millones de dólares de capital privado, Acronis continúa invirtiendo en:

- Capacidades adicionales de ciberseguridad, protección de datos y administración de endpoints
- Aprendizaje automático e inteligencia artificial para ayudar a las empresas a incrementar la automatización, la eficiencia y la capacidad de adaptación de sus planes para proteger su tiempo de actividad y sus datos
- Integración con muchos otros ISV para ampliar la funcionalidad de la plataforma a proveedores de servicios y aplicaciones verticales
- Ampliación de la presencia global y de la cantidad de centros de datos seguros en Acronis Cyber Cloud
- Promoción de Acronis Cyber Foundation, una institución sin fines de lucro que construye escuelas y ofrece formación técnica para niños y adultos con necesidades de todo el mundo

Identificar

- Inventario de software y hardware
- Clasificación de datos
- Descubrimiento de endpoints desprotegidos

Proteger

- Evaluaciones de vulnerabilidades
- Administración de parches
- Prevención de exploits
- Integración de copia de seguridad
- Control de dispositivos

Detectar

- Fuente de información de amenazas emergentes
- Búsqueda de IoC de amenazas emergentes
- Antimalware y antirransomware
- Filtrado de URL
- Seguridad del correo electrónico

Responder

- Análisis e interpretación ágiles
- Corrección de recursos informáticos con aislamiento
- Investigación remota y copias de seguridad forenses

Recuperar

- Restauración rápida de los ataques
- Preintegrada con la recuperación ante desastres
- Recuperación masiva con un solo clic
- Autorrecuperación

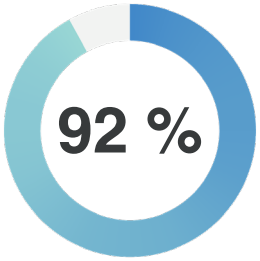
Acronis, Medalla de Oro en el cuadrante de datos, categoría de protección de endpoints, en SoftwareReviews 2022

¿Qué es el cuadrante de datos (o Data Quadrant)?

SoftwareReviews evalúa aspectos de las características y funciones del software utilizando una media ponderada de las puntuaciones del nivel de satisfacción del usuario. Estas puntuaciones emplean una escala de satisfacción para determinar si el software agrada o decepciona, creando un eficaz indicador del valor que ofrece al usuario en general.

Los clientes están muy satisfechos con Acronis y califican el software con un 8,7/10 en la puntuación compuesta. La puntuación compuesta es un promedio de cuatro ámbitos de evaluación distintos: huella emocional neta, capacidades del proveedor, funciones del producto y probabilidad de recomendación.

Tiene previsto renovar



Es probable que recomiende

"Si busca una solución que le permita aprovechar al máximo la protección, la administración y la copia de seguridad de endpoints, la ha encontrado".

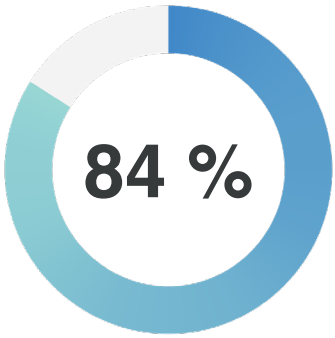
Vicepresidente de Tecnología, Electrónica

Acronis impulsa el valor de la empresa

El software de protección de endpoints permite que la organización obtenga resultados efectivos al proteger los datos, minimizar las amenazas de ransomware y garantizar la continuidad de la actividad empresarial.

Por su énfasis en la innovación para hacer frente a las amenazas modernas, su capacidad de ofrecer funciones de seguridad de próxima generación y los magníficos comentarios sobre el soporte al cliente, no debería sorprender que los clientes valoren trabajar con Acronis.

Según una puntuación de satisfacción del 84 % en cuanto al valor empresarial generado, los resultados de la encuesta demuestran que Acronis sienta las bases para que las organizaciones se protejan contra el ransomware.



Valor empresarial generado

"¡Es la mejor empresa de ciberprotección de todas! Contrátela sin pensarlo dos veces. No se arrepentirá".

Fundador, MSP

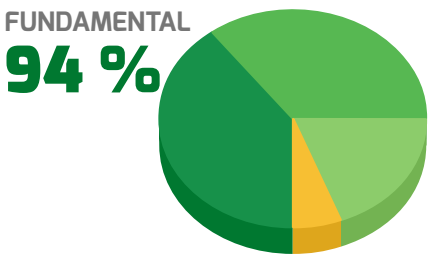
"No más noches sin dormir preocupado por las copias de seguridad. Acronis hace milagros".

Ingeniero de seguridad sénior, Servicios de TI

Acronis es una pieza fundamental del entorno de seguridad de cualquier organización

La protección de endpoints es la primera línea de defensa para proteger el entorno de la organización.

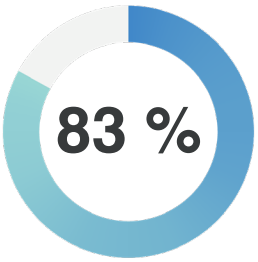
El 94 % de los clientes reconocen la importancia de Acronis para tener éxito y combatir los ataques de ransomware.



Enfoque centrado en la estrategia y la innovación para hacer frente a las amenazas modernas

La misión de Acronis consiste en proteger los datos, las aplicaciones, los sistemas y la productividad de sus clientes. Esto significa poner el énfasis en seguir desarrollando las mejores soluciones para satisfacer las necesidades de los entornos de seguridad modernos.

Acronis integra las capacidades de copia de seguridad, recuperación, antimalware de próxima generación basado en inteligencia artificial y administración de la protección en una sola solución. Con una solución en constante desarrollo diseñada para mejorar la seguridad y reducir las amenazas, no es ninguna sorpresa que Acronis se haya ubicado en el primer puesto en las categorías de estrategia de productos y tasa de mejora.



Calificada como solución líder en estrategia de productos y tasa de mejora

"Acronis es la solución de pila completa ideal. Optimiza el proceso de adición de nuevos usuarios, la seguridad general, el flujo de trabajo, la presentación de informes y la supervisión, además de hacer frente a los ataques más sofisticados con sus algoritmos complejos y sus casos de uso innovadores".

Consultor, Desarrollo de infraestructuras

Los ciberdelincuentes no dejarán de concebir nuevas maneras de acceder a sus datos, pero Acronis no dejará de concebir formas innovadoras de detenerlos

La naturaleza de las amenazas de seguridad cambia sin cesar y continuamente aparecen nuevas amenazas. Si su partner de seguridad no realiza mejoras de forma permanente, su organización puede ser vulnerable sin siquiera saber que las amenazas existen.

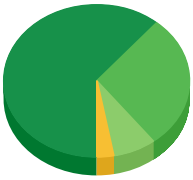
Los clientes de Acronis otorgan a la plataforma una calificación elevada por su capacidad para mejorar, inspirar, innovar y perfeccionar los productos de manera continua y en forma tal de satisfacer las necesidades de las organizaciones para mitigar posibles amenazas de seguridad y evitar ataques de ransomware.

Con el énfasis puesto en inspirar a los clientes para afrontar el entorno actual de amenazas, no debería sorprendernos que más de cinco millones de usuarios individuales y 500 000 empresas de todo el mundo confíen en Acronis.

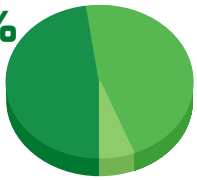
"¡Es un producto revolucionario que mejora permanentemente!"

Director gerente, Seguridad de la nube

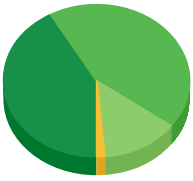
MEJORA CONTINUAMENTE
97 %



CONTRIBUYE A INNOVAR
100 %



FUENTE DE INSPIRACIÓN
99 %



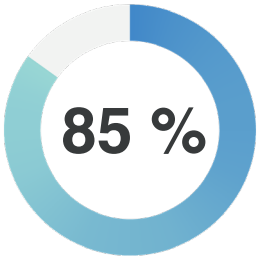
Funciones de protección de próxima generación

Al evaluar las funciones de un software de protección de datos, las organizaciones deben elegir una solución que sea compatible con los estándares y las directrices del NIST, de manera tal que los equipos de seguridad puedan alinear fácilmente sus esfuerzos en materia de ciberseguridad con los estándares del sector.

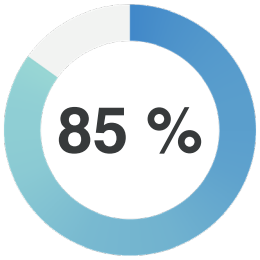
Acronis ofrece funciones de seguridad de próxima generación que son compatibles con los estándares del NIST y ayudan a los equipos de seguridad a automatizar los procesos, personalizar la plataforma según sus necesidades e integrarla sin problemas en sus sistemas existentes. Todas estas características están validadas por datos que revelan que los clientes de Acronis califican la solución de manera favorable por su calidad y por la amplitud de sus funciones.

"En cuanto a funciones y accesibilidad del producto, Acronis no tiene rival".

Desarrollo de negocios, Alimentos y bebidas



Calidad de las funciones



Amplitud de las funciones

Características principales

Detección dinámica del malware

Supervise con facilidad las posibles amenazas de seguridad aplicando a los archivos un análisis heurístico que permite identificar y bloquear el malware.

Portal de administración centralizada

Simplifique los procesos y mejore la eficiencia con herramientas para optimizar las directivas integrales, la sincronización y mucho más.

Recuperación de archivos eliminados y cifrados

Recupere sin esfuerzo los archivos que hayan sido eliminados por ataques de ransomware y acceda a los datos cifrados.

Compatibilidad entre plataformas

Asuma el control de múltiples dispositivos y sistemas operativos de los clientes con el respaldo de una única solución segura, potente y multicanal.

Fortalecimiento del sistema

Automatice los flujos de trabajo y ahorre tiempo con la evaluación de vulnerabilidades y la aplicación de parches instantáneos que las solucionan.

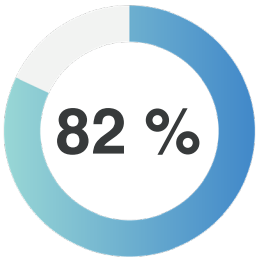
Detección y respuesta para endpoints

Haga uso del aprendizaje automático para simplificar el proceso de detectar amenazas activas y luchar contra malware conocido y desconocido.

Formación y soporte de atención al cliente efectivo

Para proteger su organización contra un ataque de ransomware, es fundamental asociarse con una solución de protección de endpoints que ofrezca un soporte al cliente de nivel superior. Acronis garantiza una experiencia de soporte al cliente excepcional de diversas maneras, a saber:

- #CyberFit Academy para acceder a formación técnica
- Foros de Acronis para participar en debates sobre productos, compartir ideas y conectar con la comunidad
- Base de conocimientos para solucionar problemas mediante el uso de guías prácticas y documentación técnica
- Equipo de soporte de Acronis para abordar los problemas de inmediato y reducir los cuellos de botella



Soporte al cliente

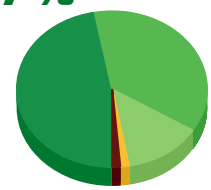
"El conjunto de funciones es increíble. Ofrece soporte de talla mundial, tanto a nivel técnico como de ventas. Todas las personas que me atendieron fueron muy amables".

Ingeniero de seguridad sénior, Servicios de TI

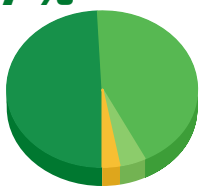
Una experiencia de soporte eficiente, respetuosa y considerada

El soporte al cliente va más allá de abordar las cuestiones técnicas de los clientes. Se trata de aportarles recursos y guiarles cada vez que necesiten ayuda, además de ofrecerles una experiencia de servicio positiva. Los datos señalan que Acronis eleva el soporte al cliente a nuevas cotas al garantizar una experiencia eficiente, respetuosa y considerada. Al poder acceder a un soporte efectivo y a materiales de capacitación, queda claro por qué los clientes otorgan a Acronis una calificación elevada en asistencia, disponibilidad y calidad de la formación.

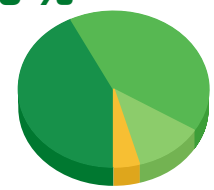
EFICIENTE
97 %



RESPETUOSO
97 %



CONSIDERADO
96 %



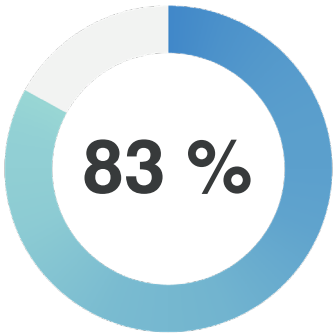
"Recomiendo cambiar a Acronis, ya que es sin lugar a dudas el mejor software de copia de seguridad que haya usado. Nuestro gerente de ventas de Acronis, que nos ayuda e instruye, nos llama una vez al mes para mantenerse informado sobre nuestra situación. No dejen de probar este excelente producto".

Gerente, Tecnología

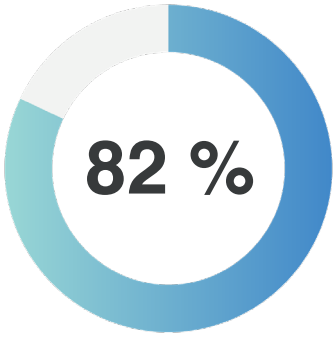
Fácil de implementar, fácil de operar

Un software de protección de endpoints que ha sido diseñado con una interfaz fácil de utilizar agiliza el tiempo de aprendizaje para los nuevos usuarios, además de ayudar a los actuales a confiar en la plataforma. Para garantizar el máximo retorno de la inversión y la mayor protección contra las amenazas de ransomware, los equipos de seguridad deben elegir una solución desarrollada en función de las necesidades del usuario final.

La plataforma de Acronis ofrece a los usuarios una interfaz sencilla, una navegación simplificada y funciones intuitivas para facilitar su adopción e implementación. La plataforma también permite que los usuarios pongan en marcha la solución antirransomware con rapidez, la integren en los sistemas existentes y la adapten según sus necesidades específicas.



Facilidad de implementación



Facilidad de administración de TI

Los comentarios de los clientes confirman que Acronis es fácil de implementar y también de utilizar. De manera más específica, los resultados de las encuestas señalan que el 83 % de los usuarios están satisfechos con la facilidad de implementación, en tanto que el 82 % lo está con la facilidad de administración de TI.

"Me encanta que Acronis supere mis expectativas. Es fácil de usar y tiene un rendimiento increíble. El editor visual facilita la integración y el uso de la plataforma para usuarios no técnicos. El conjunto de funciones es extenso y la priorización de la API permite una personalización sencilla y la ampliación de la funcionalidad. Es increíblemente sencillo".

Gerente, Tecnología

"Si desea encontrar una solución económica que ofrezca algo más que funciones de copia de seguridad y una consola centralizada fácil de usar, no busque más. Elija Acronis Cyber Protect".

Responsable de Tecnología, Proveedor de servicios de TI

Un partner a largo plazo para proteger su empresa

Cuando evalúe la asociación más conveniente a largo plazo, es importante que tenga en cuenta algunos aspectos de la solución, más allá de las funciones y del precio. Una investigación de SoftwareReviews indica que, además de cumplir con las necesidades funcionales críticas, la relación con los proveedores es lo que también contribuye al éxito a largo plazo.

La nube de palabras de SoftwareReviews registra las principales dificultades que suelen experimentarse y las opiniones más destacadas de sus usuarios. Con palabras contundentes como "confiable", "altruista" y "amigable", queda claro que los clientes tienen opiniones muy positivas sobre trabajar con Acronis.

"Es una de las mejores opciones de software de ciberseguridad con este precio. Si necesita un software de ciberseguridad confiable, debe probar Acronis".

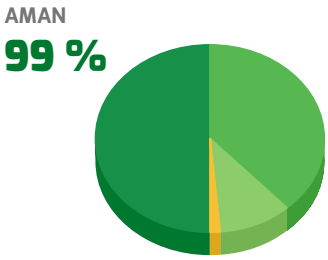
Gerente de proyectos, Tecnológica financiera

Word Cloud

Los clientes aman trabajar con Acronis

Con un producto destacado, su atención a la innovación y un excelente soporte al cliente, no debería sorprender que el 99 % de los clientes afirmen que aman trabajar con Acronis.

Para obtener más información, demostraciones del producto y una prueba gratuita, visite: www.acronis.com/es-mx/products/cyber-protect



Acerca de Acronis

Acronis unifica protección de datos y ciberseguridad para ofrecer una ciberprotección integrada y automatizada que resuelve los desafíos de seguridad, accesibilidad, privacidad, autenticidad y seguridad (SAPAS) en el mundo digital moderno. Con modelos de despliegue flexibles que responden 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 innovadoras soluciones de próxima generación antivirus, de copia de seguridad, de recuperación ante desastres y de administración de la protección de endpoints, basadas en inteligencia artificial. Gracias a su avanzado antimalware con tecnologías de vanguardia de inteligencia artificial y autenticación de datos basada en blockchain, Acronis protege cualquier entorno, ya sea en la nube, híbrido o local, por un precio reducido y previsible.

Acronis es una empresa suiza, fundada en Singapur. Cuando celebra dos décadas de innovación, Acronis cuenta con más de 2000 empleados en 45 oficinas. Las soluciones de ciberprotección de Acronis están disponibles en 26 idiomas en más de 150 países y las utilizan 16 000 proveedores de servicios para proteger a más de 750 000 empresas.

Acerca de Info-Tech Research Group y SoftwareReviews

SoftwareReviews es una división de Info-Tech Research Group, una empresa de análisis e investigación de TI de talla mundial fundada en 1997. Con dos décadas de experiencia en la investigación y la asesoría en tecnologías de la información, SoftwareReviews es líder entre las fuentes de información y experiencia en el ámbito del software para empresas y las relaciones entre clientes y proveedores.

La metodología de SoftwareReviews, que se basa en obtener datos de profesionales reales de TI y del mundo empresarial, genera información extremadamente detallada y auténtica sobre la experiencia de evaluación y compra de software empresarial.

La calidad de los datos es fundamental. Por eso SoftwareReviews hace lo imposible por garantizar que los datos que recopilamos procedan de usuarios con experiencia, de manera que le ofrezcan fiabilidad y sepa que puede tomar decisiones con confianza.

Cada revisión se verifica minuciosamente para comprobar su autenticidad a través de un proceso de control de calidad exhaustivo. Las revisiones dinámicas se adaptan según el cargo y la experiencia del revisor, para evitar suposiciones inexactas.

Acerca de la investigación

Las plataformas de protección de endpoints brindan protección contra malware, ataques de phishing y ataques de virus de manera tal de minimizar los riesgos y garantizar operaciones empresariales sin inconvenientes.

Los datos a los que hace referencia SoftwareReviews en este informe se obtuvieron de 1308 encuestados, del informe del cuadrante de datos en la categoría de protección de endpoints de agosto de 2022 y de la tarjeta de puntuación del producto Acronis Cyber Protect.

Metodología del cuadrante de datos de SoftwareReviews

SoftwareReviews recopila la información que aportan los usuarios para ayudar a las organizaciones a seleccionar de manera más efectiva un software que se ajuste a sus necesidades, medir el valor para la empresa y mejorar la selección.

Los datos y opiniones que se incluyen en este informe se obtuvieron de 1308 usuarios validados de la categoría de protección de endpoints.

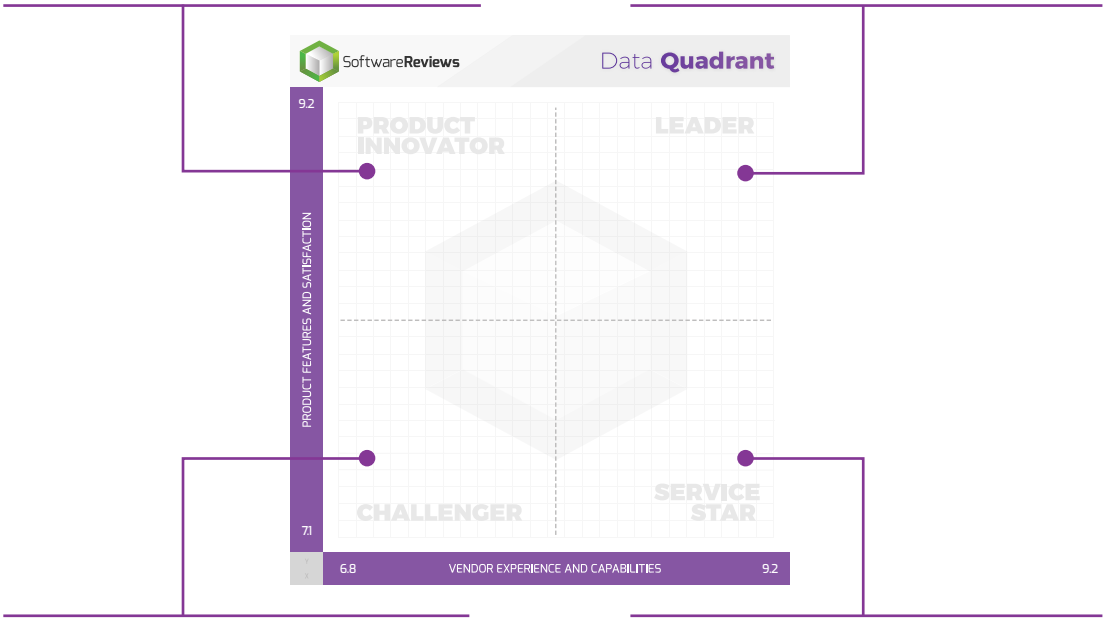
El ranking, los resultados y los puestos obtenidos en los informes de SoftwareReviews se basan exclusivamente en las opiniones de los usuarios finales solicitadas a través de un motor de encuestas online de marca registrada.

Innovadores (Product Innovators)

Productos que destacan sus funciones, por lo que obtienen buenas recomendaciones de sus clientes.

Líderes (Leaders)

Productos que más interés suscitan en el mercado y que logran igualar las funciones con una excelente experiencia del usuario.



Aspirantes (Challengers)

Productos que funcionan bien en algunas áreas, pero no tanto en otras. Por lo general, proveedores prometedores.

Estrellas del servicio (Service Stars)

Productos que priorizan una buena experiencia y desarrollan sólidas relaciones con los clientes.

Acronis