Acronis

Acronis RMM

Alcance el máximo rendimiento como MSP
con una RMM nativa, segura y con tecnología de IA integrada

Presentación del producto

Índice

Acronis

Presentación de Acronis RMM

Problemas habituales al administrar recursos hoy en día

- Sobrecarga de tareas manuales
- Escasez de talento y costes laborales
- Administración de TI reactiva
- Aumento de las ciberamenazas y de los ataques de cadena de suministro
- Fatiga por alertas
- Cumplimiento de las normativas y de las exigencias de los ciberseguros
- Problemas al administrar parches
- Entorno diversificado en múltiples herramientas

fibertel

Acronis RMM

Alcance el máximo rendimiento con una RMM nativa, segura y con tecnología de IA integrada

Integración nativa con ciberseguridad y protección de datos en una sola consola

Enfoque que da prioridad a la seguridad con funciones exclusivas de seguridad

Automatice todo, con tecnología de IA y aprendizaje automático

Incluye todo lo que necesita para ofrecer servicios de administración de TI superiores, mejorar el estado de la seguridad y aumentar el rendimiento de los técnicos

Administración de activos

- Device Sense™ para el descubrimiento de dispositivos*
- Inventario de hardware*
- Inventario de software
- Seguimiento de la geolocalización de los dispositivos.

Seguridad y cumplimiento

- Evaluaciones de vulnerabilidades
- Administración automatizada de parches
- Supervisión del firewall y del software antimalware

Supervisión y respuesta

- Supervisión de sistemas y hardware con alertas configurables
- Detección de anomalías basada en aprendizaje automático
- Acciones de respuesta automática

Automatización de tareas

- Generación de scripts asistida por IA.
- DeployPilot™ para el despliegue de software.

Soporte remoto

- Escritorio remoto y asistencia a distancia de primer nivel, integrados
- Acciones rápidas y remotas

fibertel

Alcance el máximo rendimiento mediante la automatización y la IA

Objetivos

- Aumente el número de endpoints gestionados por técnico.

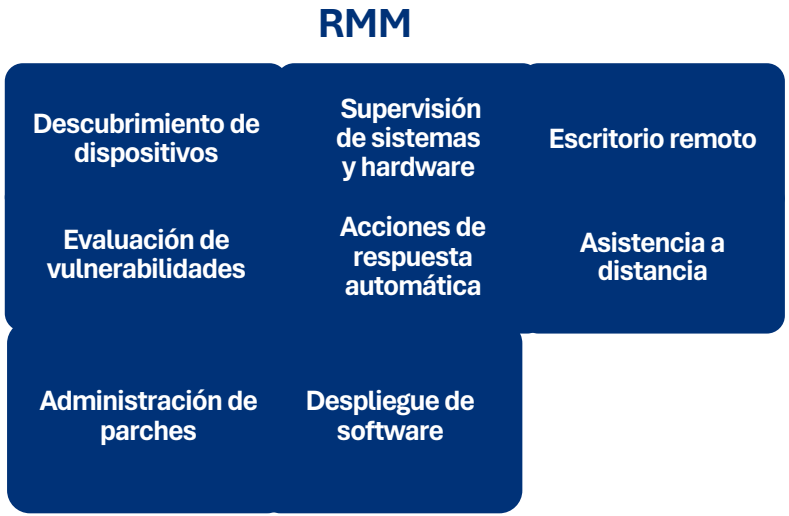
Sin necesidad de contratar personal adicional:

- Ofrezca más servicios.
- Atienda a más usuarios.
- Administre más recursos.

Cómo conseguirlo

- Ponga en piloto automático lo siguiente:
  - Evaluación de vulnerabilidades y administración de parches
  - Descubrimiento en la red
  - Acciones de respuesta ante incidentes
  - Administración de sistemas mediante la gestión de scripts
  - Despliegue de software
  - Corrección de riesgos de seguridad para Microsoft 365
- Reduzca la sobrecarga de alertas con detección de problemas basada en aprendizaje automático.
- Acelere la creación de scripts con la generación de scripts basada en IA.

Una única consola y un solo agente para todo RMM



Las integraciones nativas mejoran la protección, la fiabilidad y la eficacia

Las integraciones incorporadas entre Acronis RMM y otros servicios de Acronis permiten funciones y sinergias exclusivas.

RMM y EDR/XDR

- En la vista "Incidentes" de XDR, puede **aplicar parches a los equipos afectados** para evitar futuros ataques, **corregir los ataques** mediante generación de scripts asistida por IA, y **acceder de forma remota** a los equipos afectados para investigar los incidentes.
- Cuando despliegue software, realice análisis automáticos para detectar **malware** y **comprobaciones de firma digital**.
- **Supervise el estado** del software antimalware y del firewall.
- **Garantice la generación segura de scripts** con autodefensa frente a amenazas.

RMM + copia de seguridad y recuperación ante desastres

- **Realice copias de seguridad de los sistemas automáticamente** antes de implementar parches mediante la aplicación de parches a prueba de fallos.
- **Aplique parches y actualizaciones de software automáticamente** después de recuperar el sistema a partir de una copia de seguridad.
- **Gestione de forma proactiva los fallos de hardware** con supervisión del estado del hardware basada en aprendizaje automático y funciones de recuperación ante desastres en la nube.

RMM Y PSA

- **Simplifique la facturación** para todos los servicios de administración de endpoints. Combine los cargos por usar el software de Acronis y los costes de mano de obra en una sola factura y ofrezca opciones de facturación flexibles a los clientes.
- **Resuelva tickets con mayor rapidez:** gestione tickets y alertas, conéctese de forma remota y resuelva problemas, todo desde una sola consola.

Enfoque de Acronis con prioridad a la seguridad

- **Firme compromiso con la innovación en ciberseguridad:** a partir de la creación de su equipo de ciberseguridad en 2014, la ciberseguridad en Acronis ha evolucionado desde la introducción de Acronis Active Protection en 2017 hasta Acronis XDR en 2024.
- **Seguridad de ciclo completo:** implementa controles administrativos, físicos y técnicos rigurosos basados en las normas ISO/IEC 27000 y en el marco del NIST.
- **Desarrollo de código seguro:** integra la seguridad en el proceso de desarrollo de software mediante el marco del Ciclo de vida de desarrollo de software seguro (S-SDLC), así como formación continua en seguridad destinada a los desarrolladores.
- **Cumplimiento riguroso:** se adhiere a las normativas y reglamentos globales del RGPD y de la HIPAA, lo que garantiza el cumplimiento normativo en todas las operaciones.
- **Medidas de privacidad avanzadas:** prioriza la protección de datos y se alinea con las pautas internacionales en materia de privacidad y tratamiento seguro de información de identificación personal (PII).

fibertel

Funciones de seguridad de Acronis RMM

Generación segura de scripts

- Ejecución de scripts con autodefensa (los componentes de generación de scripts cuentan con la protección de la tecnología antimalware de Acronis).
- Autenticación de doble factor para aprobar la creación de nuevos scripts de producción y modificar los existentes.
- Registro de auditoría: se registran todas las operaciones de los scripts y se les puede realizar un seguimiento.

Supervisión de software de seguridad

- Supervisión continua de los estados del software antimalware y del firewall.

Almacenamiento seguro de credenciales

- El almacén de credenciales integrado permite almacenar credenciales de forma segura y utilizarlas tanto para ejecutar scripts como para conectarse a otros equipos a través del escritorio remoto.

Despliegue seguro de software

- Comprobaciones de firmas digitales.
- Análisis antimalware de paquetes.

Servicios de seguridad en la misma consola

- Integración nativa con Acronis XDR, antiransomware, antimalware, seguridad del correo electrónico y DLP.
- Ofrezca estos servicios desde la misma consola.

Acronis

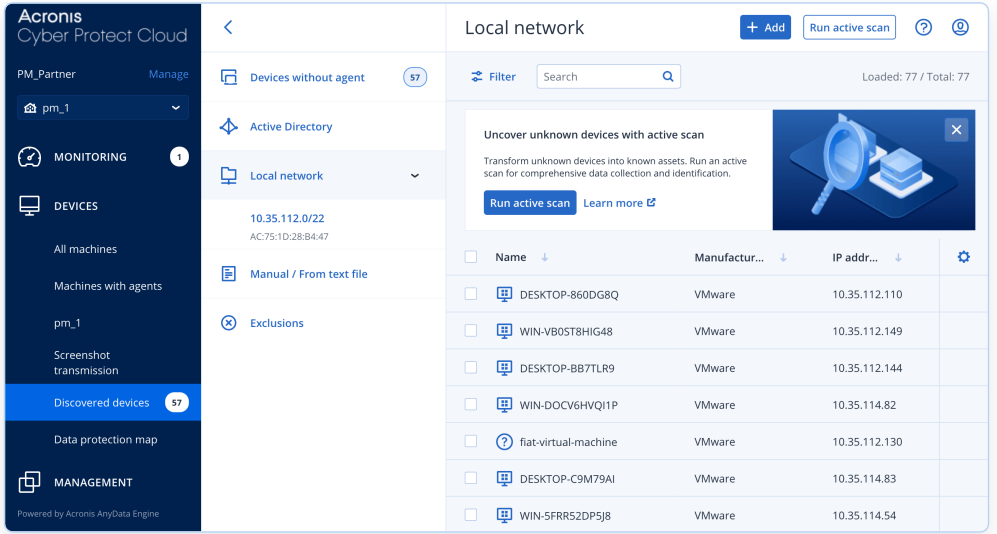
fibertel

Características principales

Descubra y proteja todos los endpoints de la red con Device Sense™

Device Sense™ es nuestra última tecnología de descubrimiento pasivo de dispositivos que le permite descubrir y proteger los endpoints de los clientes de forma ininterrumpida.

- **Detecte** todos los dispositivos, desde servidores y estaciones de trabajo hasta smartphones, tablets y dispositivos de conexión a redes virtuales como routers, switches e impresoras.
- **Identifique** estos dispositivos y obtenga información detallada sobre ellos, lo que garantiza una gestión de inventarios precisa y útil.
- **Proteja** todos los recursos informáticos de inmediato y a gran escala: instale agentes automáticamente e implemente planes de protección.
- **Lleve a cabo análisis pasivos continuos** para obtener una lista completa y actualizada de todos los dispositivos.
- **Lleve a cabo análisis activos bajo demanda** para recopilar datos detallados sobre los dispositivos.

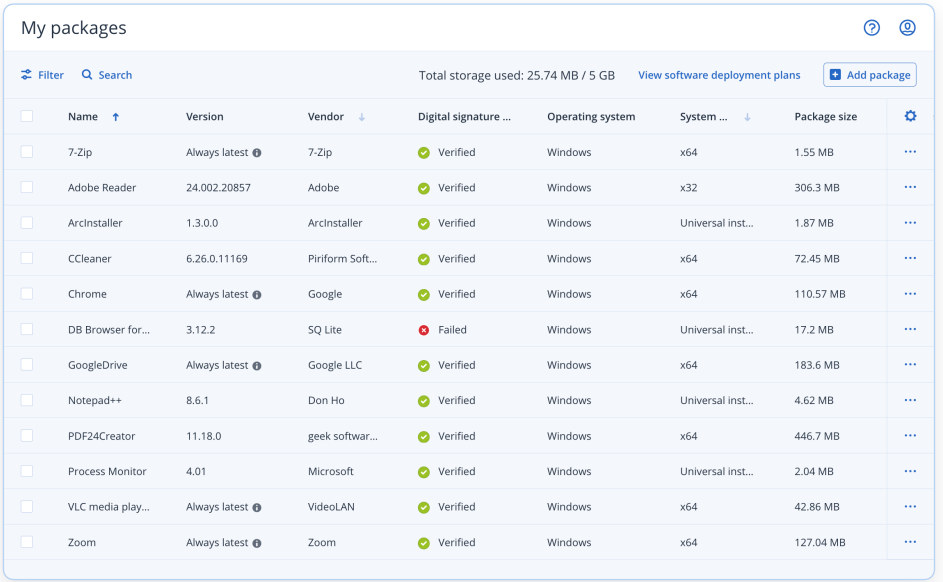


Automatice todos los aspectos del despliegue de software y la administración de parches

Centralice y automatice el despliegue de software en todos los entornos de sus clientes gracias a DeployPilot™

El despliegue de software en Acronis RMM permite a los administradores de TI gestionar despliegues de forma remota y a gran escala.

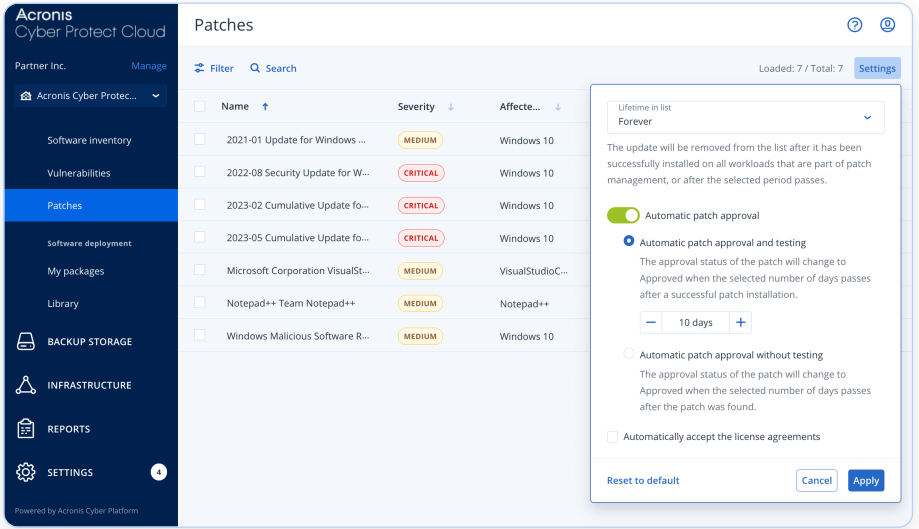
- **Exclusivo:** cree repositorios de software que incluyan tanto paquetes probados por Acronis, procedentes de una biblioteca seleccionada de aplicaciones de uso general, como paquetes de despliegue personalizados.
- Repositorios **centralizados tanto para varios clientes como para clientes individuales.**
- **Exclusivo: garantice la seguridad** con comprobaciones automáticas de firmas digitales y análisis antimalware de paquetes.
- **Active el despliegue remoto masivo de software** en varios dispositivos de diferentes ubicaciones simultáneamente.
- **Automatice el despliegue con opciones flexibles** para instalaciones planificadas, recurrentes y activadas mediante eventos.
- **Garantice el cumplimiento normativo y mejore la satisfacción de los clientes** con alertas en tiempo real, paneles de control de estado y registros de auditoría.



Ponga la administración de parches en piloto automático

Mejore la productividad de los técnicos y la seguridad de los clientes con funciones automatizadas de evaluación de vulnerabilidades y administración de parches.

- **Evaluación de vulnerabilidades automática** para todos los sistemas operativos principales: Windows, macOS y Linux.
- **Administración de parches automatizada** para más de 300 aplicaciones Windows de uso general.
- **Exclusivo: tecnología de administración de parches patentada y fiable** con copias de seguridad automáticas antes de aplicar los parches.
- **Aplique parches a los sistemas automáticamente tras la recuperación** desde una copia de seguridad.
- **Visibilidad y control centralizados** en todos los entornos de los clientes.



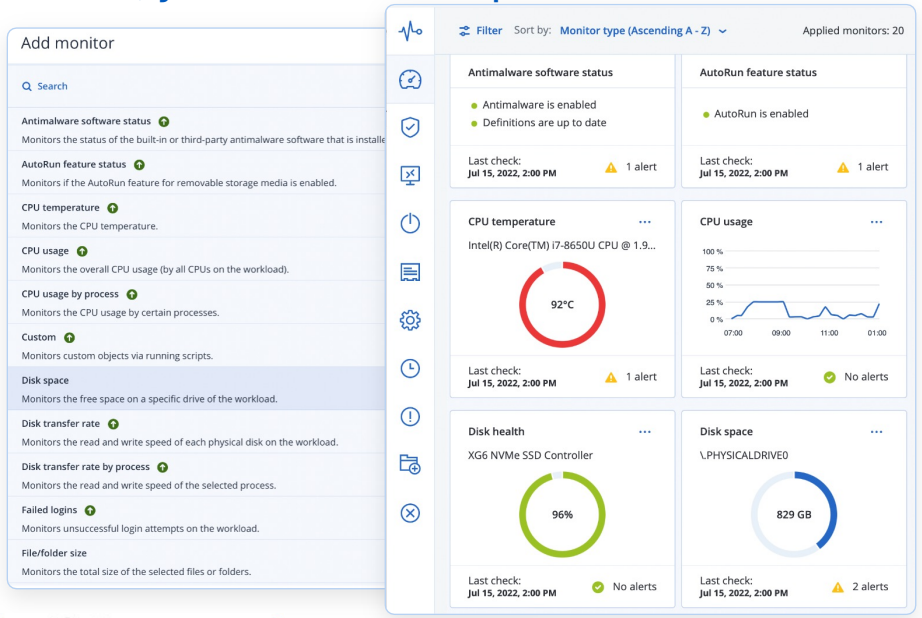
"Ahora, gracias a Acronis (...) podemos aplicar parches con un solo clic a todos los ordenadores online. Ahora me basta con unos 2-5 minutos para aplicar todos los parches, cuando antes necesitaba dos días enteros". **Vladimir Georieski, CEO, JVS Net**

fibertel

Habilite una administración de TI proactiva y preventiva con supervisión basada en aprendizaje automático y acciones de respuesta automática

Supervisión del rendimiento del sistema y del hardware con alertas basadas en anomalías y en umbrales, supervisores predefinidos y personalizados, y acciones de respuesta automática.

- **Habilite una administración preventiva de TI con supervisión de sistemas y hardware basada en anomalías** que predice los problemas antes de que ocurran y causen daños.
- **Supervise de forma proactiva más de 20 parámetros de sistemas y hardware**, así como otros parámetros personalizados para Windows y macOS, con el fin de identificar posibles problemas con antelación.
- **Acelere la resolución de problemas con respuestas automáticas** a las alertas: ejecución de scripts, reinicio de servicios y ejecución de acciones de respuesta.
- **Reduzca la sobrecarga de alertas de los técnicos** gracias a una mayor precisión en la detección de problemas, reglas de alerta precisas y acciones de respuesta automática.

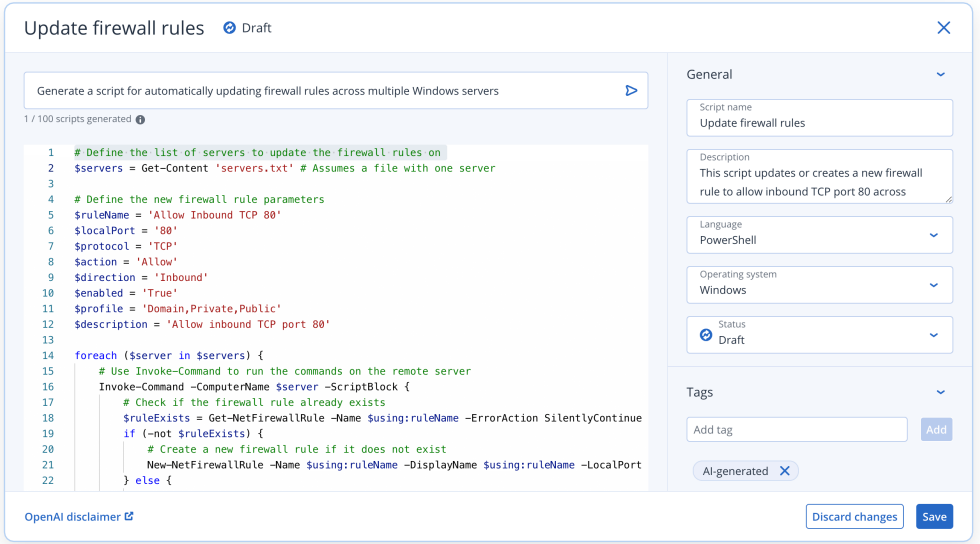


fibertel

Automatice las operaciones de TI rutinarias con generación de scripts asistida por IA

Automatice tareas para equipos Windows y macOS, incluidas la administración de sistemas y la gestión de archivos, usuarios y redes, con el fin de reducir el esfuerzo manual y minimizar el riesgo de que se produzcan errores humanos.

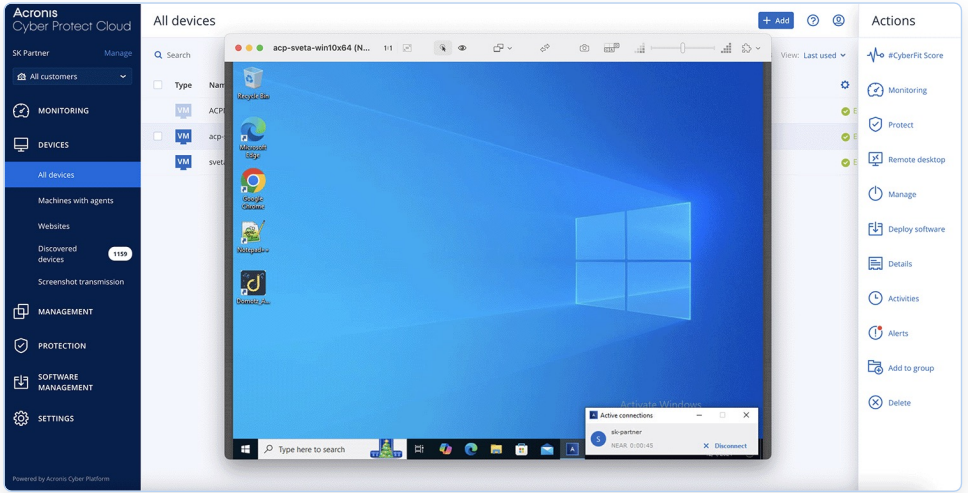
- Aproveche la generación y edición de scripts basada en IA para aumentar la productividad y reducir los errores humanos, gracias a nuestra integración con OpenAI.
- Despliegue y ejecute scripts en varios clientes y endpoints, con administración centralizada de scripts.
- Aumente la escala para satisfacer las crecientes demandas de sus clientes, con despliegues a gran escala y entornos de TI complejos.
- **Exclusivo:** automatice flujos de trabajo de respuesta ante incidentes de seguridad a través de la integración con Acronis XDR.
- **Exclusivo:** reduzca el riesgo de infecciones por malware y evite ataques basados en scripts con la ejecución segura de scripts, que incluye mecanismos de autodefensa.



Obtenga escritorio remoto y asistencia a distancia: funciones seguras, de alto rendimiento y sin coste adicional

Proporcione asistencia remota, rápida y segura con una solución de escritorio remoto integrada, disponible desde la misma consola.

- **Simplifique la administración, reduzca los costes de formación y otros costes**: la asistencia y escritorio remotos están integrados, utilizan el mismo agente de Acronis y no requieren licencias adicionales.
- **Ofrezca soporte para todos los sistemas operativos:** Windows, macOS y Linux.
- **Realice acciones remotas,** como reiniciar el sistema, poner el dispositivo en suspensión y vaciar la papelera de reciclaje.
- **Exclusivo: proporcione soporte al instante e inicie una conexión con cualquier endpoint,** incluso sin un agente instalado, a través de Quick Assist.
- **Exclusivo: permita el acceso remoto a equipos en cuarentena** afectados por un ciberataque directamente desde la interfaz de XDR para llevar a cabo una investigación y corrección inmediatas.*



* Requiere tener Acronis EDR/XDR habilitado.

Acronis

fibertel

Resumen

Cambiar a Acronis RMM desde otras soluciones de RMM ofrece varias ventajas

Mejore la seguridad, eficacia y fiabilidad

con integraciones nativas en RMM, PSA, ciberseguridad y protección de datos.

Mejore la seguridad de los clientes

con el enfoque de Acronis, que da prioridad a la seguridad, y mediante amplias funciones de seguridad.

Atienda a clientes que no hablan inglés

con un producto localizado en 25 idiomas.

Recorte costes

al incluir un escritorio remoto de primer nivel sin coste adicional.

Almacene los datos de los clientes en centros de datos locales

Acronis opera una red de decenas de centros de datos a nivel global.

Ofrezca administración de TI proactiva y preventiva

con supervisión de sistemas y hardware basada en anomalías.

Reduzca la sobrecarga de alertas

con detección de problemas basada en aprendizaje automático.

fibertel

Si Acronis RMM es su primer RMM, obtendrá las siguientes ventajas:

Automatice las tareas rutinarias

para permitir a los técnicos gestionar más recursos y resolver problemas con mayor rapidez.

Ahorre costes

con una sola licencia para todas las herramientas de RMM.

Escale con facilidad

a medida que su empresa crezca, con un solo agente unificado por equipo cliente.

Disminuya la necesidad de visitas in situ

y permita resolver más problemas de forma remota, con el fin de reducir costes e invertir menos tiempo en desplazamientos.

Resuelva los problemas de los clientes antes de que se conviertan en críticos

mediante funciones de supervisión proactiva y preventiva.

Mejore los tiempos de respuesta y la calidad del servicio

al reforzar la confianza y la retención de los clientes.

fibertel

Acronis

fibertel

Detalles de la función

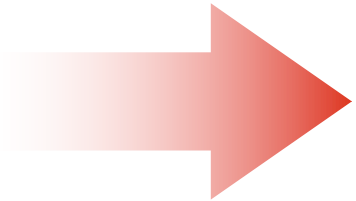
Acronis

fibertel

Device Sense™

La necesidad de disponer de una mejor solución para descubrir y proteger todos los dispositivos en la red

Visibilidad insuficiente de todos los dispositivos conectados a la red del cliente debido a un seguimiento manual o ineficaz de los dispositivos



Vulnerabilidades de seguridad

Riesgos en el cumplimiento de normativas

Riesgos en el cumplimiento de ciberseguros

Inventario impreciso y desactualizado

Asignación ineficaz de recursos

fibertel

Device Sense™

Device Sense™ es una tecnología diseñada para descubrir, identificar y proteger todos los dispositivos de la red de un cliente de forma ininterrumpida, lo que mejora la visibilidad, la seguridad y el cumplimiento normativo.

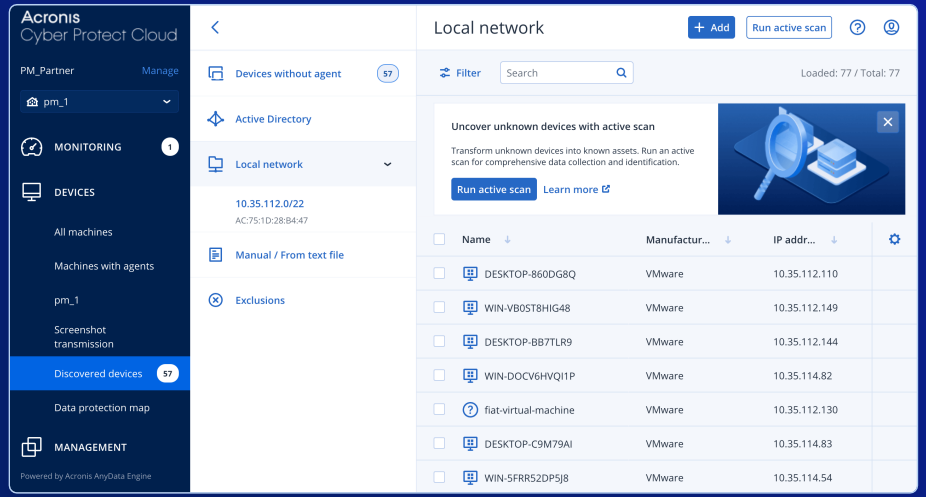
- **Detecte** todos los dispositivos, desde servidores y estaciones de trabajo hasta smartphones, tablets y dispositivos de conexión a redes virtuales como routers, switches e impresoras.
- **Identifique** estos dispositivos y obtenga información detallada sobre ellos, lo que garantiza una gestión de inventarios precisa y útil.
- **Proteja** todas las cargas de trabajo de inmediato y a gran escala mediante el programa de instalación de agentes y la aplicación de planes de protección, supervisión y administración remota.

Licencias

Disponible como parte de la versión estándar de Acronis Cyber Protect Cloud.

Doble análisis exhaustivo

Combina **escaneo pasivo continuo** (para obtener una lista completa y actualizada de todos los dispositivos) con **escaneo activo bajo demanda** (para recopilar datos en profundidad sobre estos dispositivos).



Mejora de la visibilidad, la seguridad, el cumplimiento y los ingresos

Mejor visibilidad de las redes

- Consiga una supervisión total de todos los dispositivos conectados a las redes de sus clientes, desde servidores y ordenadores portátiles hasta hardware de red.

Mayor seguridad

- La identificación de cada recurso informático, junto con la aplicación inmediata de planes de protección, garantiza la seguridad de cualquier nuevo recurso informático que se conecte a la red de un cliente, lo que minimiza el riesgo de sufrir posibles vulnerabilidades.

Cumplimiento de normativas y de exigencias de ciberseguros

- Mantenga automáticamente un inventario actualizado y completo, y garantice la protección de todos los recursos informáticos de la red para ayudar a sus clientes a cumplir con las normativas de cumplimiento más estrictas.

Aumento de ingresos

- Amplíe la oferta de servicios y aumente los ingresos por cliente al proteger y gestionar más recursos informáticos.

Asignación eficaz de recursos

- Gestione de forma estratégica los recursos técnicos y reduzca los costes gracias a una visión completa del ámbito de las redes de sus clientes.

Administración remota simplificada

- Instale agentes y aplique planes de gestión de forma rápida y en masa, al agilizar las operaciones, mejorar la prestación de servicios y aumentar la seguridad.

Más allá del descubrimiento: un conjunto completo de funciones

Análisis pasivo continuo

Para obtener una lista completa y siempre actualizada de los dispositivos.

Análisis activo bajo demanda

Para recopilar datos más detallados sobre dichos dispositivos.

Descubrimiento de dispositivos en la red

Descubra todos los dispositivos en la red, incluidas las estaciones de trabajo, teléfonos, routers e impresoras.

Prevención de análisis en redes no corporativas

Evite ejecutar análisis en entornos domésticos o no corporativos.

Gestión de inventario

Examine los dispositivos detectados con opciones avanzadas de búsqueda y filtrado.

Instalación de agente remota

Instale los agentes de Acronis en todos los equipos Windows con unos pocos clics.

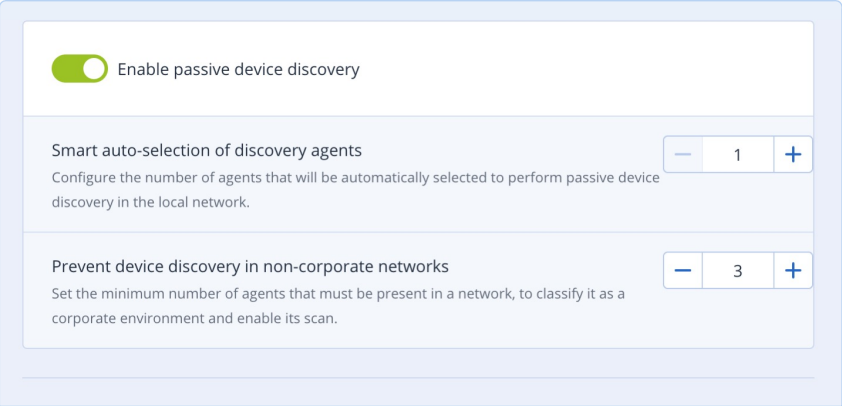
Aplicación de planes de protección

Aplique planes de protección, supervisión y administración a gran escala para todos los equipos.

Generación de informes detallados

Genere informes sobre los dispositivos descubiertos, lo que facilita la administración de la red y el cumplimiento de las normativas.

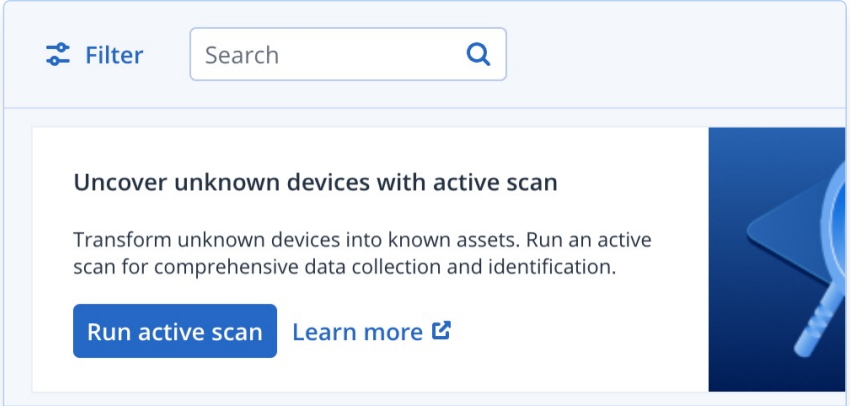
Doble análisis exhaustivo



Análisis pasivo continuo

El análisis pasivo es un método no intrusivo que se utiliza para identificar y catalogar los dispositivos en un entorno de red, sin sondear de forma activa la red de la organización y sin enviar solicitudes a los dispositivos conectados a dicha red.

Los datos que se recuperan mediante el análisis pasivo incluyen los siguientes: el nombre y tipo de dispositivo, la familia del sistema operativo, el fabricante, el modelo, la dirección MAC y la dirección IP.



Análisis activo bajo demanda

El análisis activo es un método que se utiliza en la administración de redes, en el que un sistema sondea o se comunica activamente con los dispositivos de una red para identificarlos y recopilar información sobre ellos.

Permite recuperar datos más completos y precisos sobre los dispositivos, por lo que complementa la información recopilada mediante el descubrimiento pasivo.

Prevención de análisis en redes no corporativas

EXCLUSIVO

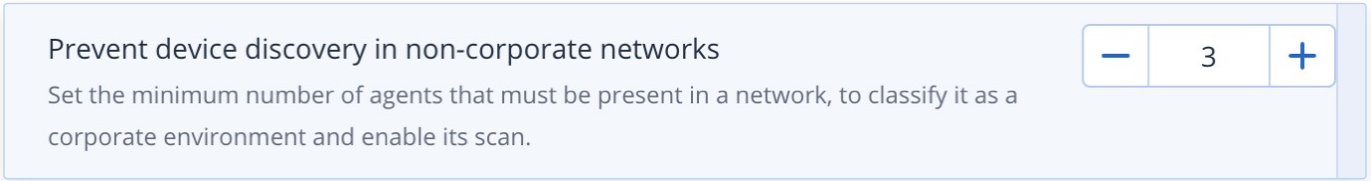
Evite ejecutar análisis en entornos domésticos o no corporativos

El problema:

Analizar accidentalmente redes no corporativas puede dar lugar a la recopilación innecesaria de datos y a posibles problemas relacionados con la privacidad.

La solución:

Device Sense™ incorpora una función distintiva que evita el descubrimiento de dispositivos en redes virtuales no corporativas. Una red se clasifica como corporativa en función de la presencia de un número especificado de agentes de Acronis. Los administradores pueden definir este umbral en la configuración de descubrimiento de dispositivos para que se ajuste a sus directivas de protección. De forma predeterminada, el umbral se establece en tres agentes, lo que garantiza que solo se analicen las redes con una presencia corporativa suficiente. Este enfoque específico evita añadir dispositivos no corporativos al inventario y mantiene los estándares de privacidad.



fibertel

Acronis

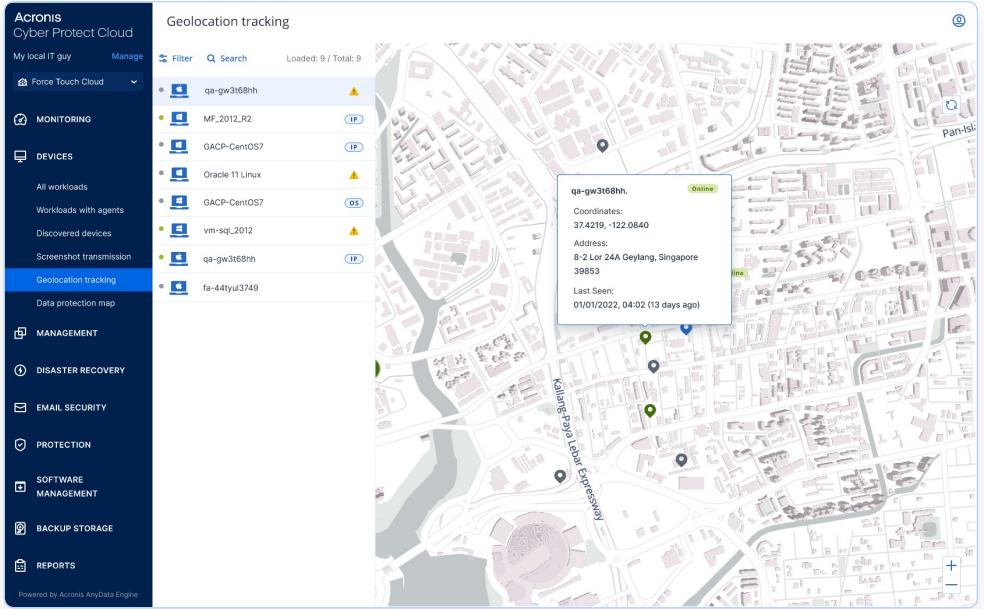
Otras funciones de administración de recursos

Seguimiento de la geolocalización de los dispositivos

NOVEDAD

Garantice el cumplimiento normativo y reduzca el tiempo de inactividad gracias al seguimiento de la geolocalización de los recursos de TI de sus clientes

- **Realice un seguimiento de los dispositivos para mantenerlos en ubicaciones autorizadas** y cumplir con los requisitos internos y normativos.
- **Localice y recupere los dispositivos perdidos o robados**, lo que no solo minimiza las posibles interrupciones para los clientes, sino que también reduce el tiempo de inactividad de las empresas.
- **Optimice la asignación de recursos para los técnicos que trabajen in situ** al asignarles tareas en función de su ubicación en tiempo real, lo que mejorará los tiempos de respuesta y la eficacia del personal.
- **Soporte para dos métodos de geolocalización:** geolocalización basada en sistemas operativos para obtener una mayor precisión y geolocalización basada en direcciones IP para disfrutar de mayor compatibilidad.
- Compatible con **Windows**, **macOS** y **Linux**.



fibertel

Inventario de hardware

Tenga siempre información actualizada sobre los recursos de hardware para planificar las sustituciones de manera adecuada

Aumente la visibilidad con información actualizada sobre los recursos de hardware:

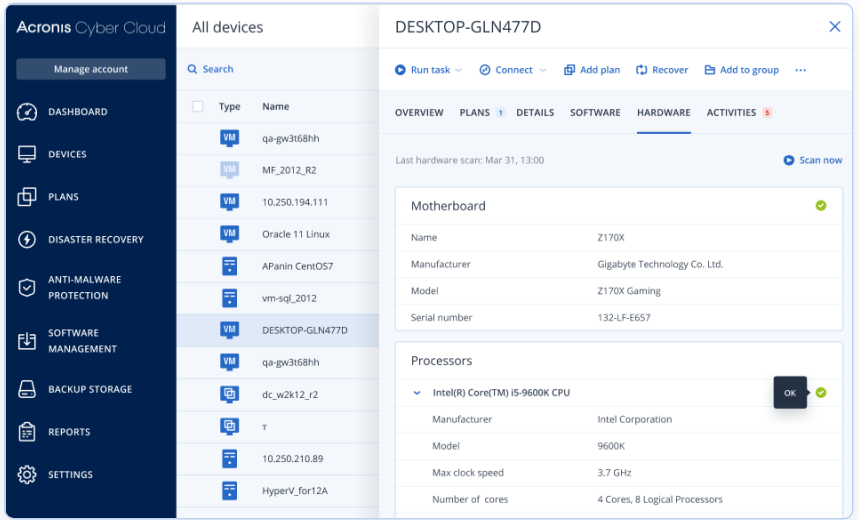
- Descubra todos los recursos de hardware en todos los equipos registrados de la organización (p. ej., CPU, GPU, tarjeta madre, RAM, adaptadores de red, etc.)
- Análisis automatizados planificados o bajo demanda

Consiga una planificación más eficiente con información detallada sobre los recursos de hardware, como el modelo, fabricante, número de serie, etc.

- Información principal del hardware de la lista de todas las máquinas
- Información detallada de hardware en los detalles de cada máquina
- Haga búsquedas de todos los recursos de hardware o busque y filtre en función de varios criterios: modelo de procesador, núcleos del procesador, tamaño total del disco, capacidad de memoria, etc.

Simplifique el mantenimiento y facilite la planificación

- Controle los cambios en los recursos de hardware y genere informes de inventario de hardware
- Elimine automáticamente los registros una vez que se elimine una máquina o inquilino



¿Por qué? Ahorro de tiempo y esfuerzo, y simplificación de la planificación de sustitución de recursos.

Inventario de software

Lista completa del software utilizado por sus clientes, para planificar y controlar las actualizaciones de forma eficaz

Aumente la visibilidad con información actualizada sobre todos los recursos de software:

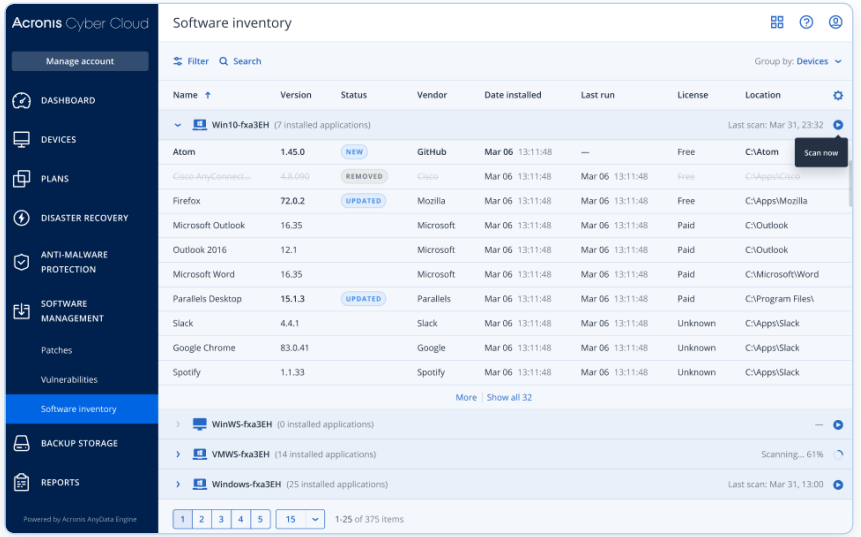
- Descubra todos los recursos de software en todos los equipos registrados en la organización
- Planifique análisis automatizados o ejecútelos bajo demanda

Mejore la productividad con la opción de examinar todos los recursos de software que se muestran en la consola de Acronis Cyber Protect:

- Todos los endpoints u ordenadores registrados en la consola
- Endpoints u ordenadores específicos
- Busque y filtre los recursos de software según múltiples criterios (nombre del software, proveedor de software, estado)

Reduzca el tiempo dedicado a tareas de mantenimiento:

- Controle los cambios en el inventario de software y genere informes de inventario de software
- Elimine automáticamente los registros una vez que se elimine una máquina o inquilino



¿Por qué? Ahorro de tiempo y esfuerzo al preparar, planificar o controlar las actualizaciones.

Acronis

fibertel

DeployPilot™

Problemas de los MSP que se resuelven al desplegar software

- Sobrecarga por instalaciones manuales
- Limitaciones de escalabilidad
- Visitas in situ
- Errores de configuración
- Versiones de software incoherentes
- Falta de visibilidad y control
- Tiempo de inactividad operativo
- Riesgos de seguridad y autenticidad

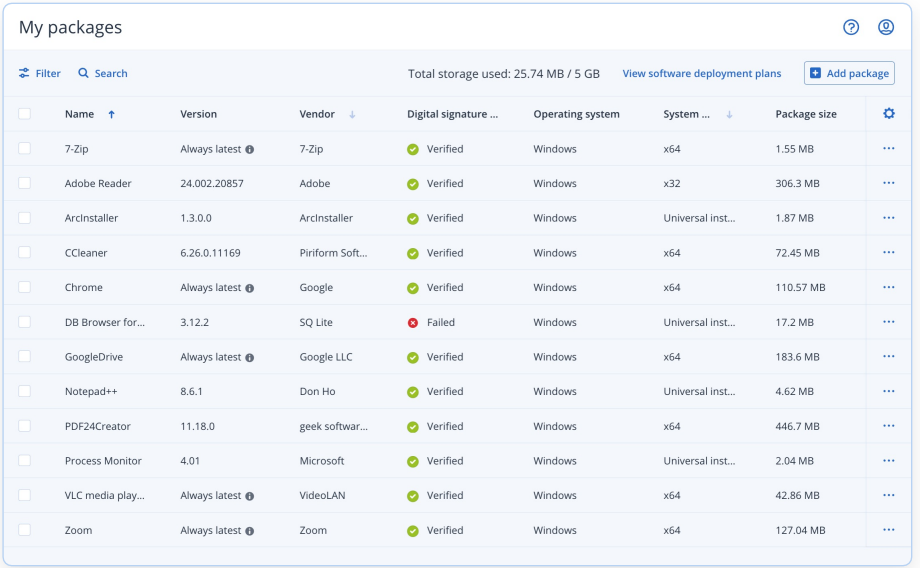
fibertel

DeployPilot™

Centralice y automatice el despliegue de software en todos los entornos de sus clientes

DeployPilot™ permite a los MSP y a los administradores de TI gestionar despliegues de software de forma remota y a gran escala.

- **Logre tanto la estandarización como la personalización** al crear repositorios de software con paquetes probados por Acronis, procedentes de una biblioteca seleccionada, y con aplicaciones personalizadas. Los repositorios pueden ser tanto centralizados y comunes a varios clientes, o por cliente individual.
- **Garantice la seguridad** con comprobaciones automáticas de firmas digitales y análisis antimalware de paquetes.
- **Despliegue software de forma masiva desde una única consola** a varios dispositivos en diferentes ubicaciones simultáneamente.
- **Automatice el despliegue con opciones flexibles** para instalaciones planificadas, recurrentes y activadas mediante eventos.
- **Garantice el cumplimiento normativo y mejore la satisfacción del cliente** con alertas en tiempo real, paneles de control de estado y registros de auditoría.



Automatice todos los aspectos del despliegue de software y la administración de parches

Acronis

fibertel

Características principales

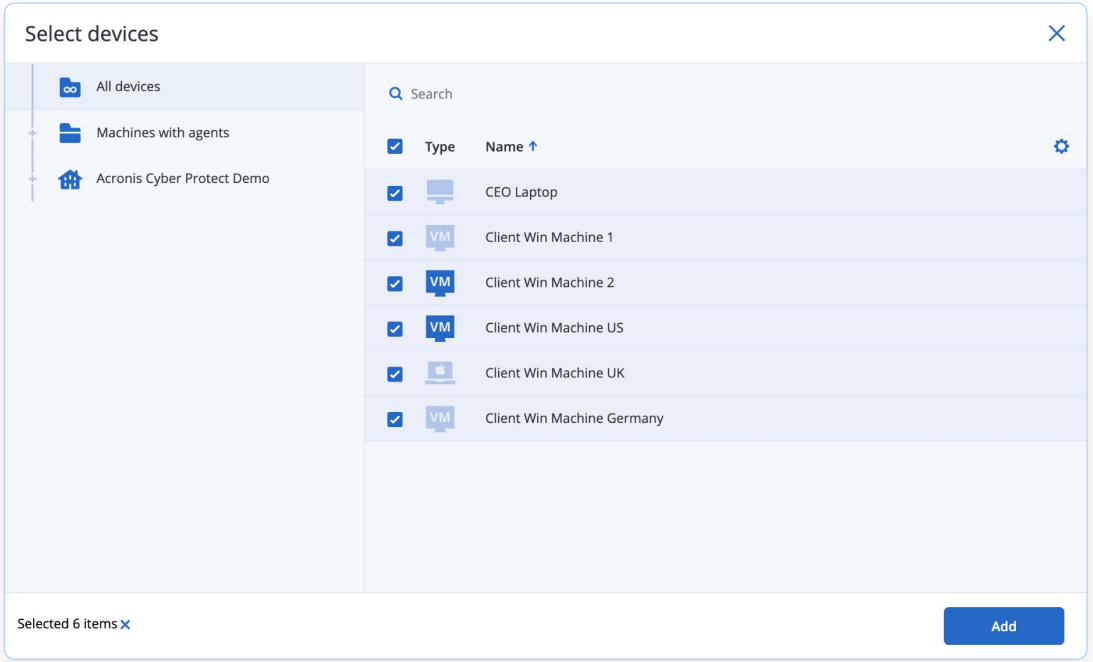
Administración remota

Despliegue masivo de software desde una consola centralizada:

Despliegue software en varios dispositivos de distintas ubicaciones simultáneamente.

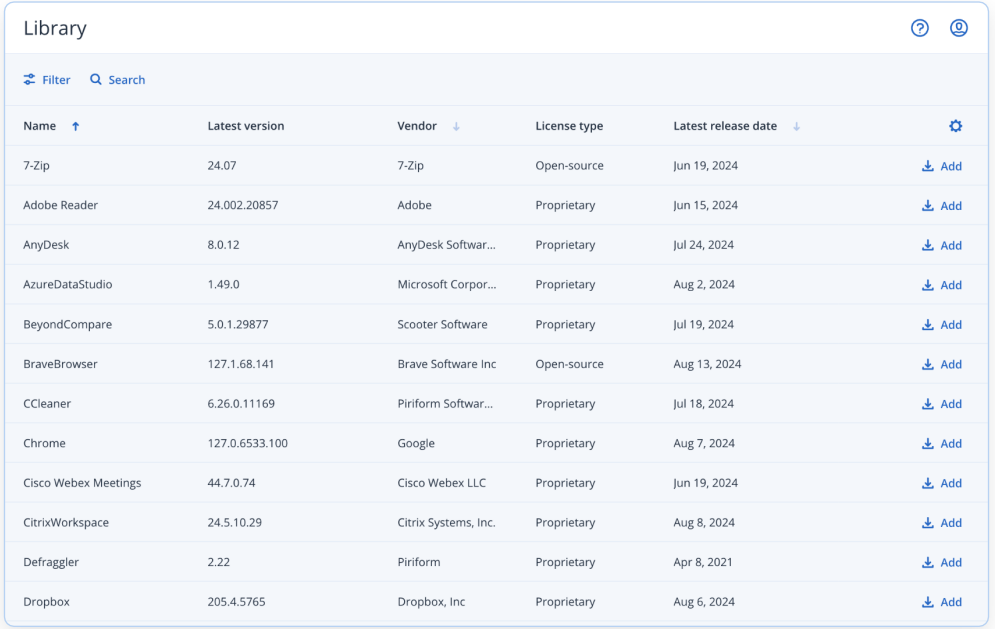
Elimine la necesidad de realizar instalaciones manuales o visitas in situ.

Ahorre tiempo y reduzca costes.



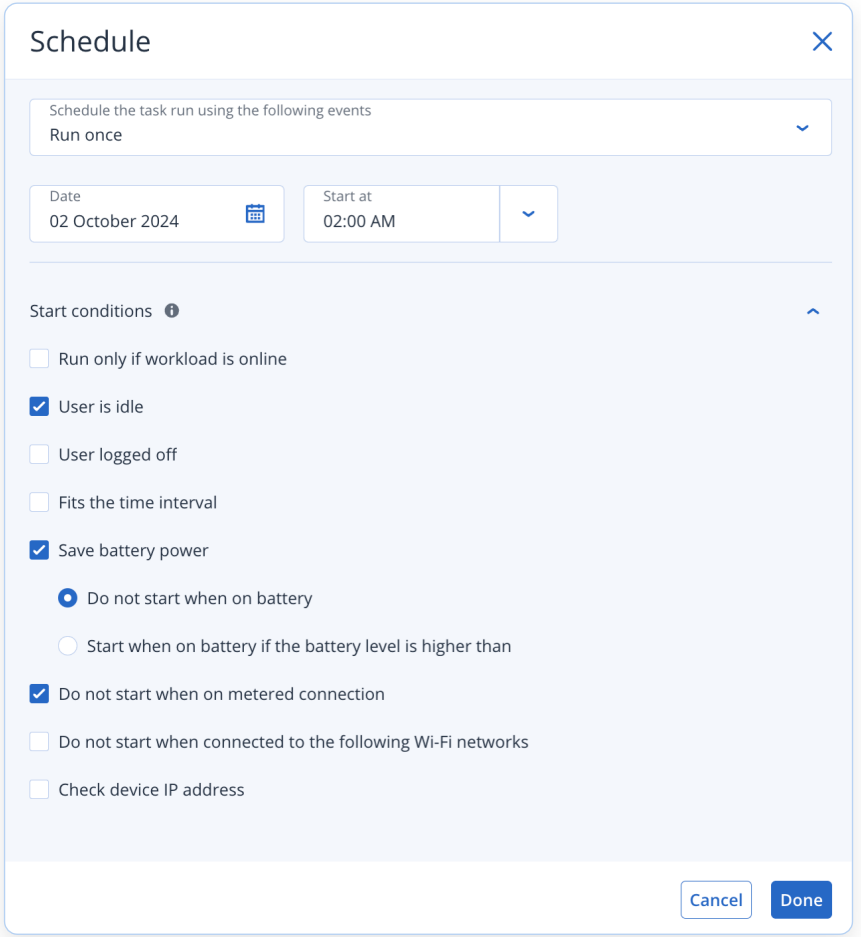
Repositorios y paquetes de software

- **Biblioteca seleccionada por Acronis:** un repositorio de paquetes listos para desplegar y probados por Acronis para un despliegue rápido y una mayor fiabilidad.
- **Soporte para aplicaciones personalizadas y creadas internamente:** cargue paquetes de software de otras fuentes para satisfacer las necesidades específicas de cada cliente.
- **Actualizaciones automáticas de paquetes:** los paquetes importados de la biblioteca de Acronis se mantienen actualizados de forma automática, lo que reduce el mantenimiento manual.
- **Repositorio "Mis paquetes":** cree repositorios personalizados que contengan paquetes tanto de la biblioteca de Acronis como de otras fuentes.
- **Repositorios centralizados tanto para varios clientes como para clientes individuales:** para estandarizar los despliegues entre clientes y, al mismo tiempo, mantener la flexibilidad.



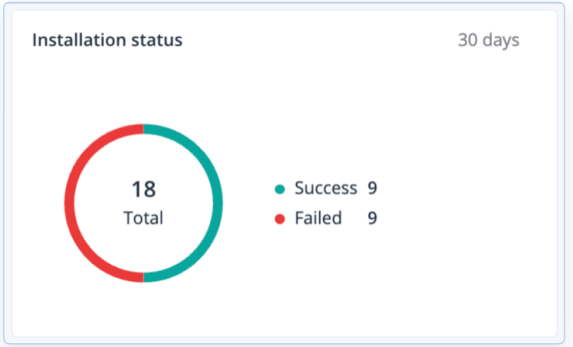
Opciones de despliegue

- **Despliegue bajo demanda:** ofrece la opción de "desplegar ahora" para llevar a cabo el despliegue inmediato de software en los equipos seleccionados.
- **Despliegues programados y recurrentes:** permite que los despliegues de software se ejecuten una vez en el futuro o se repitan diaria, semanal o mensualmente.
- **Despliegues activados mediante eventos:** activa automáticamente despliegues en función de determinados eventos, como el inicio o apagado del sistema o el inicio de sesión de un usuario.



Supervisión, generación de informes y cumplimiento de normativas

- **Alertas:** proporciona notificaciones en tiempo real sobre el estado del despliegue y posibles problemas.
- **Paneles de control:** ofrece estadísticas sobre los despliegues realizados correctamente o con errores, así como el historial de instalación y desinstalación de todos los equipos.
- **Registros de auditoría:** mantiene registros detallados de todas las actividades de despliegue con fines de seguimiento y cumplimiento normativo.



Software installation history — 30 days

Machine name	Software name	Vendor name	Version	Installation date	Software plan	Signature check status	Installation status
Sw-Dep-VM2	Zoom	Zoom	6.1.6.43767	02.10.2024	Test installation	Verified	Success
Sw-Dep-VM1	Process Monitor	Microsoft	4.01	01.10.2024	Software deploymen...	Verified	Failed
Sw-Dep-VM1	Notepad++	Don Ho	8.6.1	01.10.2024	Software deploymen...	Verified	Failed
Sw-Dep-VM1	ArcInstaller	ArcInstaller	1.3.0.0	01.10.2024	Software deploymen...	Verified	Failed
Sw-Dep-VM1	Process Monitor	Microsoft	4.01	24.09.2024	Software deploymen...	Verified	Failed
Sw-Dep-VM1	Notepad++	Don Ho	8.6.1	24.09.2024	Software deploymen...	Verified	Failed
Sw-Dep-VM1	ArcInstaller	ArcInstaller	1.3.0.0	24.09.2024	Software deploymen...	Verified	Failed
Sw-Dep-VM1	Zoom	Zoom	6.1.6.43767	24.09.2024	Software deploymen...	Verified	Success
Sw-Dep-VM1	VLC media player	VideoLAN	3.0.21	24.09.2024	Software deploymen...	Verified	Success
Sw-Dep-VM1	Process Monitor	Microsoft	4.01	24.09.2024	Software deploymen...	Verified	Failed

More

fibertel

Acronis

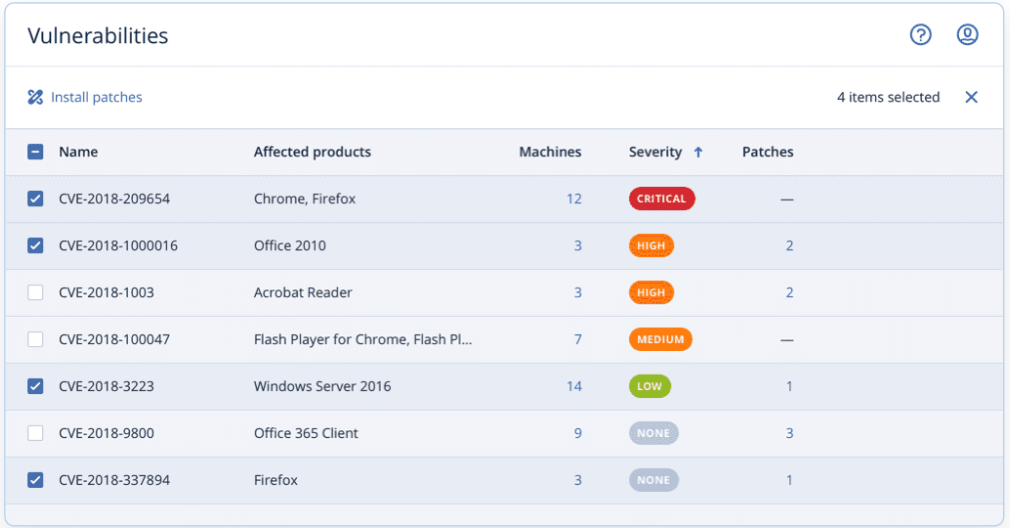
fibertel

Administración de parches y evaluaciones de vulnerabilidades

Evaluaciones de vulnerabilidades

Descubra los problemas antes de que ocurran

- Compatibilidad con Windows, macOS y Linux
- Actualizaciones diarias continuas de nuestra propia base de datos de administración de parches y vulnerabilidades
- Panel integral para detectar vulnerabilidades, evaluar su gravedad y controlar la disponibilidad de los parches



Compatibilidad con **más de 300** apps de terceros y con todas las apps de Microsoft

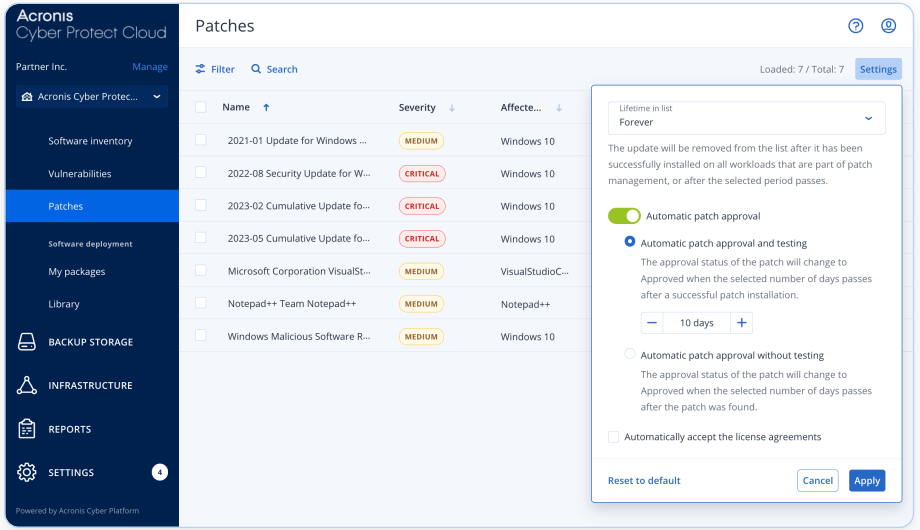
¿Por qué? Mitigación de las amenazas potenciales y prevención de ataques.

Administración de parches

Garantice la protección de endpoints

Amplia base de datos de vulnerabilidades y riesgos comunes (CVE), con 250-300 nuevas incorporaciones cada semana

- **Todas las actualizaciones de Windows,** incluidas Microsoft Office y las apps de Windows 10
- Compatibilidad con administración de parches de **software de Microsoft y de terceros** en Windows
- **Copias de seguridad previas a la actualización** y aplicación de los últimos parches como parte del proceso de **recuperación**.
- Visibilidad de la **prioridad de los parches**, en función de la gravedad de la vulnerabilidad
- Aplicación de parches prioritarios para **aplicaciones de colaboración:** Zoom, Skype, Microsoft Teams, Cisco Webex, etc.
- Despliegue **por fases** para probar los parches



¿Por qué? Mitigación de las amenazas potenciales y prevención de ataques (como los de Equifax o WannaCry).

N.º 1 en compatibilidad de productos en Windows

Proveedor	Número de productos admitidos
Acronis	**Más de 300**
Panda	189
Ivanti	152
Bitdefender Cloud Security for MSP	146
NinjaOne	135
Symantec	95
Kaspersky	94
F-Secure	75
Automox / SentinelOne	36
SolarWinds	34
ConnectWise	11

Las cifras se basan en fuentes públicas. No se puede garantizar un 100 % de precisión.

Seguridad integral

Ofrece una protección más amplia frente a las vulnerabilidades y reduce el riesgo de que se produzcan brechas de la seguridad.

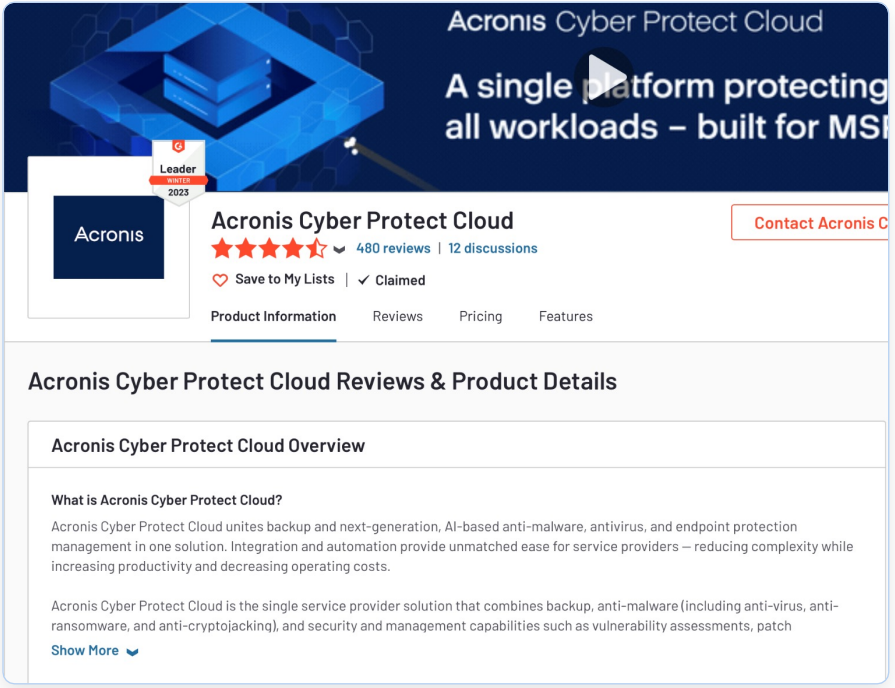
Eficacia operativa

Simplifica la administración de parches automatizada mediante la automatización de una amplia gama de software, lo que ahorra tiempo y recursos a los MSP.

Ventaja competitiva

Cobertura para una amplia variedad de aplicaciones, lo que se traduce en un aumento de la captación de clientes y de los niveles de satisfacción de los mismos.

Líder en la cuadrícula de administración de parches G2



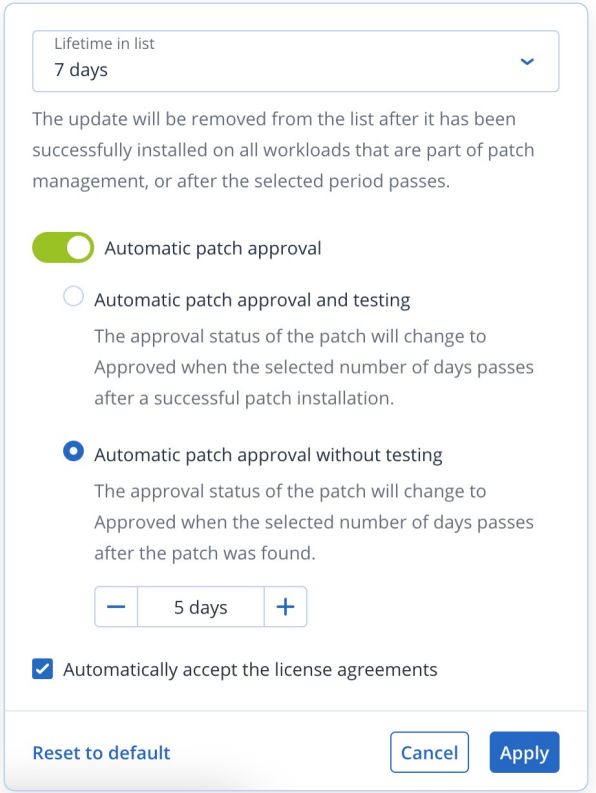
G2 Grid® para la administración de parches
https://www.g2.com/categories/patch-management#grid

fibertel

Automatización de la administración de parches

Cierre automático de vulnerabilidades antes de que las aprovechen los ciberdelincuentes

- **Aprobación automática** de parches:
  reduzca el personal necesario para operar
- Despliegue según una **planificación**:
  planifique y automatice la administración de parches
- Opciones **flexibles** de tiempo de reinicio y mantenimiento:
  minimice el tiempo de inactividad planificado



¿Por qué? Administración de parches automatizada para simplificar las operaciones.

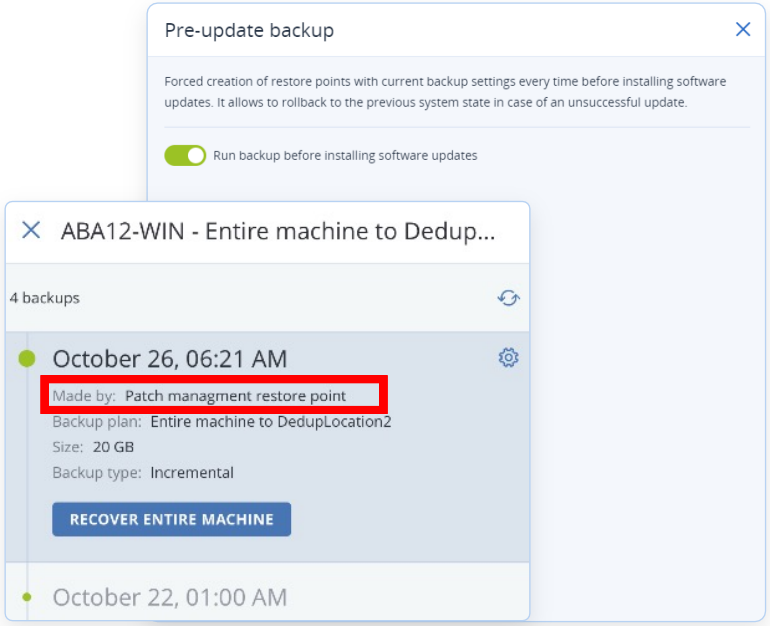
fibertel

Aplicación de parches a prueba de fallos

Función exclusiva de Acronis

Haga una copia de seguridad automática de los endpoints antes de aplicar los parches para permitir la reversión rápida al estado de funcionamiento

El **88 %** de las empresas afirman que aplicarían los parches más rápidamente si tuvieran la opción de anularlos inmediatamente en caso necesario.



Un parche inadecuado puede inutilizar los sistemas. Las reversiones de parches tienen limitaciones y pueden ser lentas. Cree una copia de seguridad de imagen de los equipos seleccionados antes de instalar un parche de un sistema o aplicación.

Las copias de seguridad de imagen completa son la forma más rápida y fácil de revertir un sistema a un estado utilizable.

Fuente: Informe de la encuesta de 0patch, 2018

¿Por qué?

Ahorro de recursos, minimización del tiempo de inactividad y operaciones más rápidas y fiables.

Acronis

fibertel

Supervisión de sistemas y hardware

Supervisión basada en aprendizaje automático y alertas inteligentes

Mitigue los riesgos operativos y optimice la supervisión

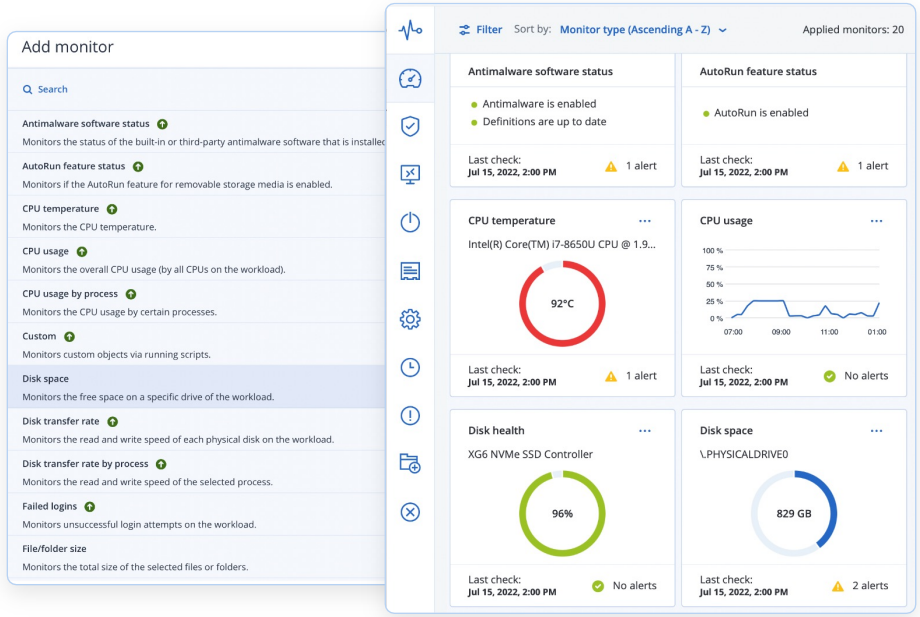
La supervisión basada en aprendizaje automático y las alertas inteligentes aumentan la eficiencia de los técnicos de TI gracias a la detección de anomalías de manera automática, rápida y precisa, y a las medidas automáticas de respuesta.

Los técnicos de TI pueden adoptar un enfoque proactivo para la protección de los clientes, de manera que conozcan el rendimiento y la fiabilidad de los equipos y puedan gestionar más endpoints con menos esfuerzo, en lugar de tener que supervisar multitud de alertas, múltiples consolas y varias herramientas complejas.

La supervisión basada en aprendizaje automático permite gestionar equipos Windows y macOS.

Ejemplos de tareas típicas:

- Supervisión del estado del software antimalware integrado o de terceros
- Supervisión de la velocidad de lectura y escritura de cada disco físico
- Supervisión del tráfico entrante y saliente para cada adaptador de red



¿Por qué?

Los partners pueden reducir el número de alertas generadas y aplicar medidas de corrección automáticas.

Mitigue los riesgos operativos y optimice la supervisión

Supervise el rendimiento y la fiabilidad de los equipos

Evalúe el estado de cualquier equipo y, a continuación, cuando se alcance un umbral específico, realice una acción.

Aumente su eficiencia

Reduzca la pérdida de tiempo y proporcione soporte de confianza mediante una detección de anomalías predictiva, precisa y automática, con acciones de respuesta automáticas.

Reduzca el número de alertas generadas

Personalice la gravedad, la frecuencia y los mensajes de las alertas. Reciba alertas en la consola de Acronis Cyber Protect solo cuando los parámetros controlados estén fuera del límite normal.

Ventajas de la supervisión basada en aprendizaje automático y de las alertas inteligentes

Previsión

Supervisión basada en aprendizaje automático y alertas con detección predictiva en tiempo real para aplicar respuestas rápidas y automáticas.

Automatización

Solución automática de las alarmas detectadas en función de plantillas de corrección, sin la intervención de un técnico.

Precisión

Supervisión de parámetros de rendimiento (hardware, software, servicios, procesos y eventos críticos) en equipos remotos con reglas definidas manualmente y modelos de inteligencia automática, para alertar y aplicar las medidas de corrección de manera más rigurosa.

Mayor compatibilidad

Supervisión de 24 parámetros/métricas para equipos Windows y macOS.

Parámetros de supervisión disponibles

ID	Función	Producto estándar	Advanced Management
Supervisión basada en aprendizaje automático y alertas inteligentes			
1	Estado del software antimalware	NO	SÍ
2	Estado de la función de ejecución automática	NO	SÍ
3	Temperatura de la CPU	NO	SÍ
4	Uso de la CPU	NO	SÍ
5	Uso de la CPU por proceso	NO	SÍ
6	Personalizado	NO	SÍ
7	Espacio en disco	SÍ	SÍ
8	Velocidad de transferencia del disco	NO	SÍ
9	Velocidad de transferencia del disco por proceso	NO	SÍ
10	Inicios de sesión fallidos	NO	SÍ
11	Tamaño de archivos y carpetas	SÍ	SÍ
12	Estado del firewall	NO	SÍ
13	Temperatura de la GPU	NO	SÍ

ID	Función	Producto estándar	Advanced Management
Supervisión basada en aprendizaje automático y alertas inteligentes			
14	Cambios en el hardware	SÍ	SÍ
15	Software instalado	NO	SÍ
16	Último reinicio del sistema	SÍ	SÍ
17	Uso de memoria	NO	SÍ
18	Uso de memoria por proceso	NO	SÍ
19	Uso de red	NO	SÍ
20	Uso de red por proceso	NO	SÍ
21	Estado del proceso	NO	SÍ
22	Estado de actualización de Windows	NO	SÍ
23	Registro de eventos de Windows	NO	SÍ
24	Estado de servicio de Windows	NO	SÍ

Acronis

fibertel

Generación de scripts asistida por IA

Generación de scripts asistida por IA

Automatice operaciones rutinarias de TI para equipos con Windows y macOS, tales como:

- Realización de pasos de remediación, acelerando la resolución de problemas y minimizando el tiempo de inactividad para los clientes.
- Estandarización de configuraciones en los endpoint de los clientes.
- Automatización de configuraciones de seguridad para responder ante incidentes de seguridad: mejora en las defensas de los clientes contra posibles ciberataques.
- Automatización de la instalación de software en miles de equipos de clientes.

Esta automatización reduce considerablemente el esfuerzo manual y minimiza el riesgo de error humano.

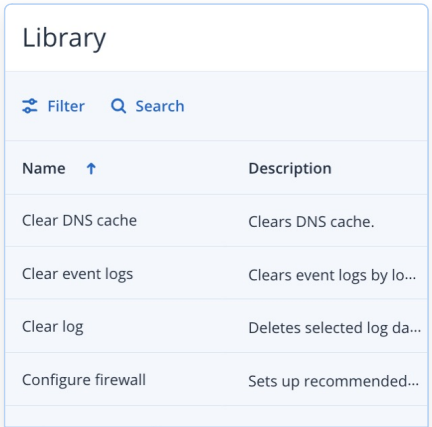
Con IA

Apóyese en OpenAI para crear rápidamente scripts de PowerShell y Bash, lo que mejorará la eficiencia y reducirá aún más los errores humanos.

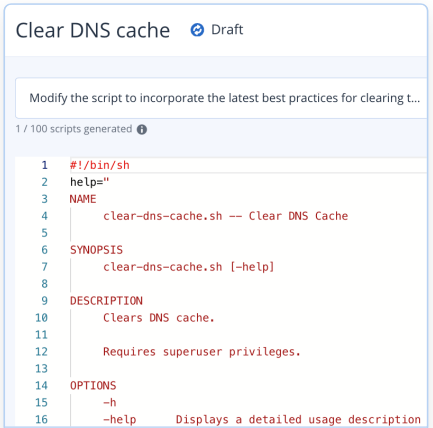
Segura

El mecanismo de autodefensa, impulsado por el motor anti-malware de Acronis, protege los componentes de ejecución de scripts contra la inyección o intercepción de código malicioso.

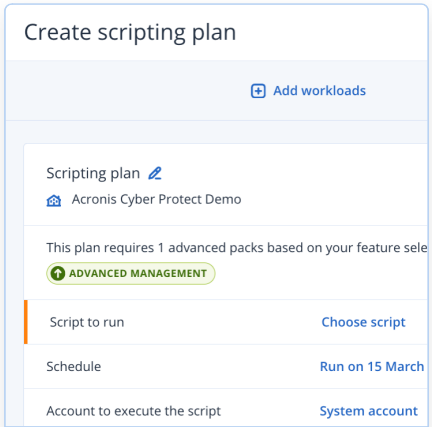
Otras funciones principales



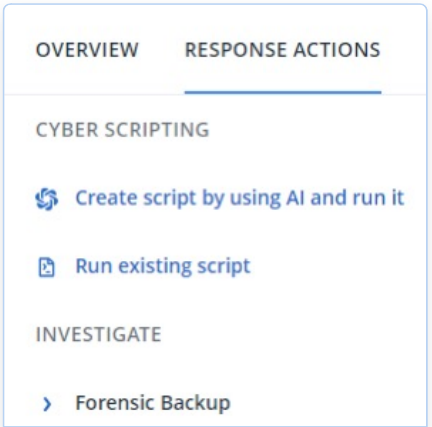
Más de 40 scripts predefinidos y verificados para tareas comunes.



Refinación de scripts existentes manualmente o utilizando IA.

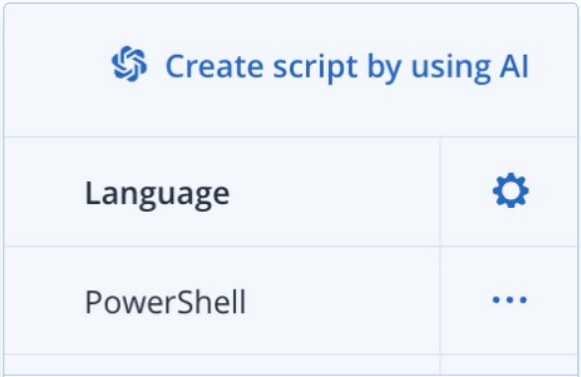


Planes de ejecución de scripts para automatización escalable y personalizable.



Integración con Advanced Security + EDR para acciones de respuesta inmediata.

Scripts basados en IA: escenarios clave

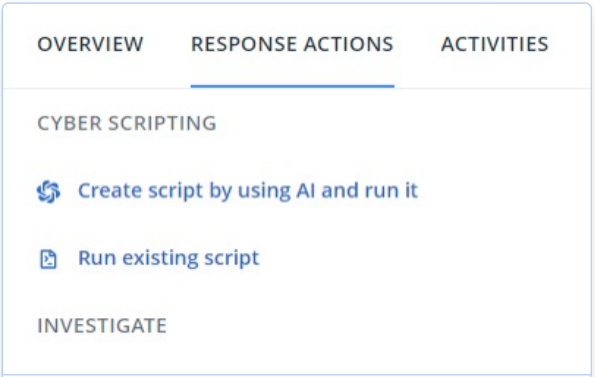


Generación de scripts con tecnología de IA

La interfaz intuitiva se adapta a todos los niveles de experiencia técnica. Los usuarios pueden introducir un conjunto de instrucciones, y la IA genera un script personalizado adaptado a esos requisitos.

Mejoras de scripts preexistentes

Para requisitos más complejos, donde ya existan scripts parciales, se completan estos scripts según las instrucciones que se indiquen. Además, incluye comentarios en línea para comprender los scripts de forma precisa.



Integración con Advanced Security + EDR

En caso de sufrir algún incidente de seguridad, los técnicos pueden generar scripts con rapidez a través de la IA directamente desde la consola de Advanced Security + EDR para llevar a cabo acciones de mitigación inmediatas.

Ventajas de utilizar scripts generados por OpenAI

Conocimientos de programación

OpenAI entiende una amplia gama de lenguajes de programación y herramientas de TI, lo que le permite crear fragmentos de código relevantes y precisos rápidamente.

Eficacia para cualquier tarea compleja

Acelera la codificación de tareas simples y complejas; puede utilizarse como punto de partida o como solución para scripts listos para usarlos en producción.

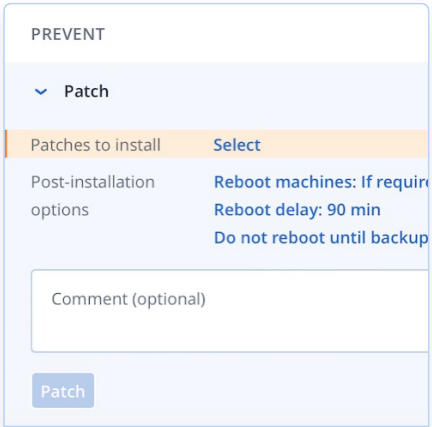
Reducción de errores

Minimiza los errores de codificación con una sintaxis y lógica precisas. Verifica la corrección del código generado y sugiere mejoras o alternativas.

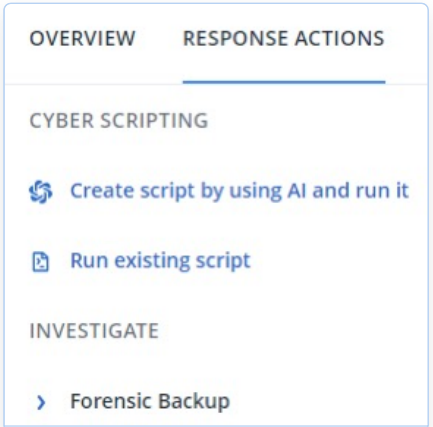
Procesamiento de lenguaje natural

Traduce instrucciones en inglés en código ejecutable, comprendiendo de forma inteligente los requisitos y las intenciones.

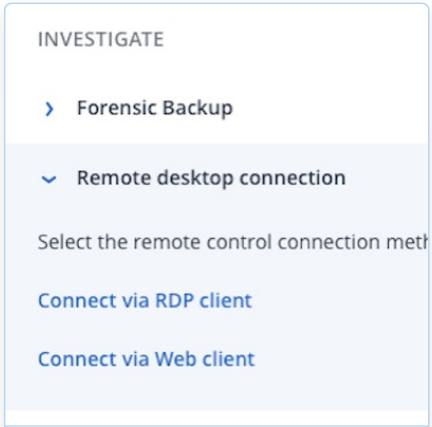
Cómo Acronis RMM mejora la seguridad mediante la integración con Advanced Security + EDR/XDR



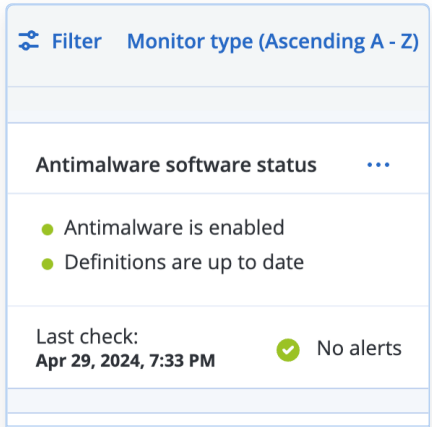
Aplicación de parches a gran escala y por equipo



Corrección rápida mediante scripts asistidos por IA



Conexión mediante escritorio remoto para investigar los ataques sufridos



Supervisión del estado del software antimalware y del firewall

Acronis

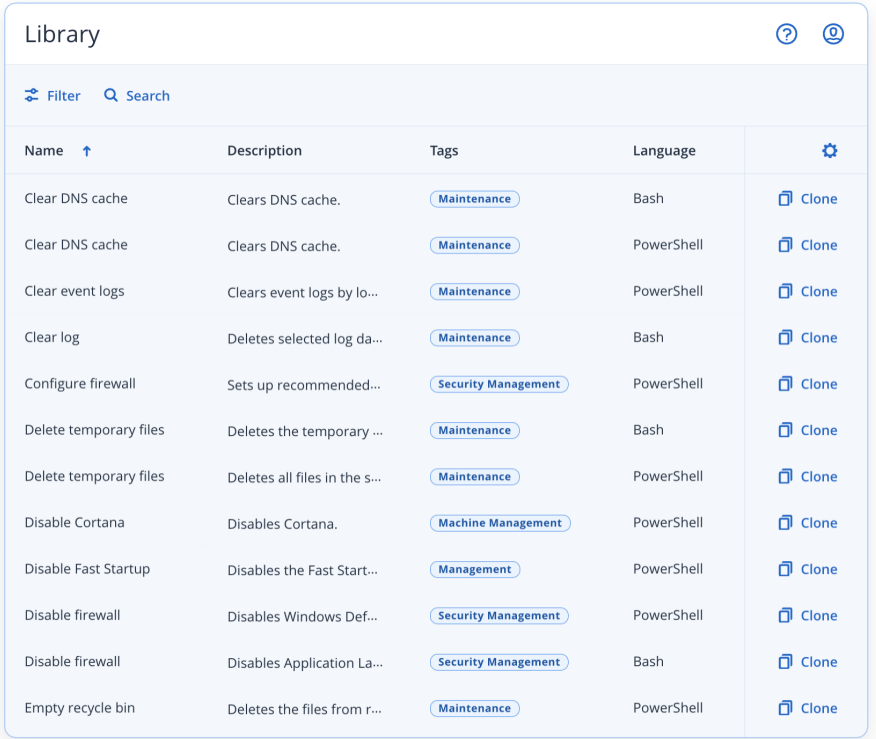
fibertel

Otras funciones de generación de scripts basada en IA

Una biblioteca de scripts predefinidos

Aproveche una biblioteca de scripts verificados por Acronis y personalizables

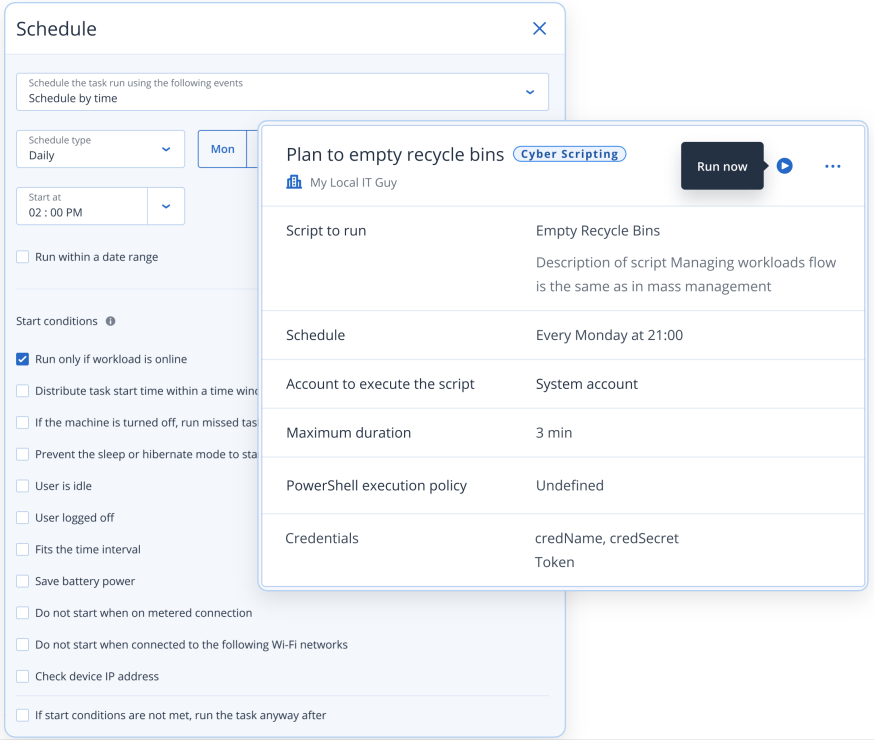
- Acceda a una biblioteca de más de 40 scripts verificados por Acronis que puede ejecutar en cualquier grupo de equipos.
- Ajuste las tareas de script existentes o cree y mantenga scripts personalizados para los clientes.
- Personalice y ajuste los scripts manualmente o mediante IA.



Planes de generación de scripts para administración escalable

Simplifique las operaciones con ajustes detallados de planificación y ejecución de scripts

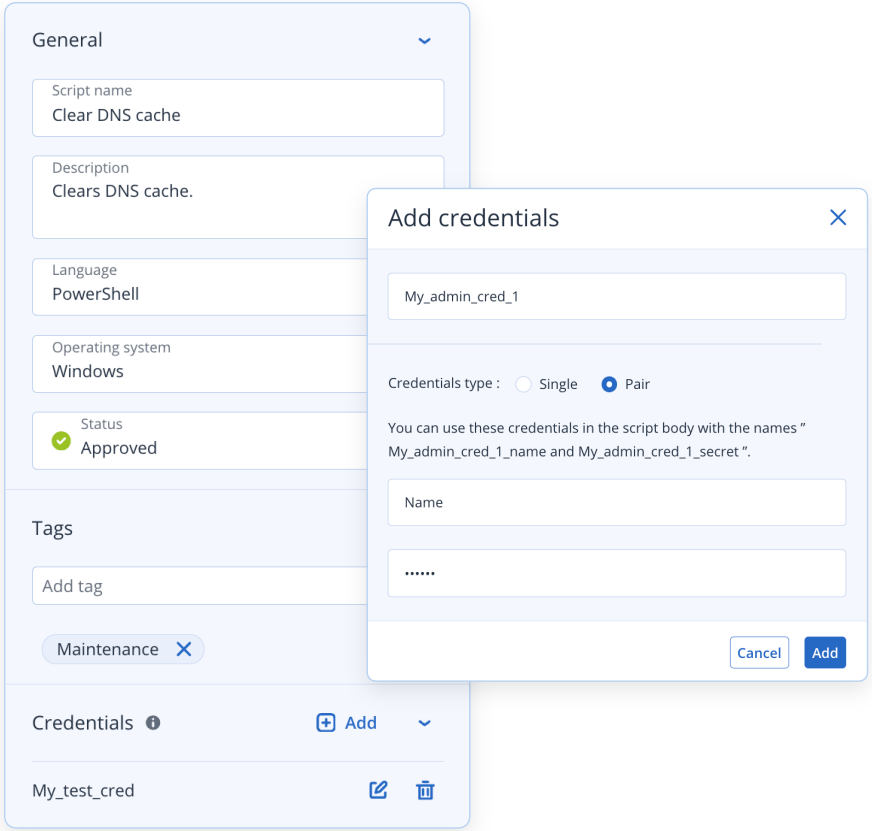
- Planificación detallada de las ejecuciones de scripts o tareas inmediatas bajo demanda, con el fin de mejorar la eficacia operativa mediante la elección de los mejores momentos para ejecutar los scripts.
- Ejecución instantánea de scripts, según se haya planificado:
  - Ejecuciones repetitivas.
  - Ejecuciones puntuales.
  - En función de las condiciones de inicio específicas, como la activación del equipo, intervalos de tiempo o inactividad de los usuarios.
- La integración de la administración de credenciales en las directivas de generación de scripts, así como la opción de establecer una duración máxima de ejecución de los scripts, garantizan operaciones seguras y eficaces sin riesgo de sobrecarga del sistema.



Generación segura de scripts

Autodefensa para la ejecución segura de scripts

- El motor antimalware integrado evita que las amenazas maliciosas afecten a la ejecución de los scripts.
- La autenticación de doble factor garantiza la seguridad del proceso de aprobación de scripts nuevos o modificados en producción.
- El almacén de credenciales integrado permite a los partners almacenar credenciales de forma segura.
- El registro de auditoría integrado permite realizar un seguimiento y registrar todas las operaciones de los scripts.



Acronis

fibertel

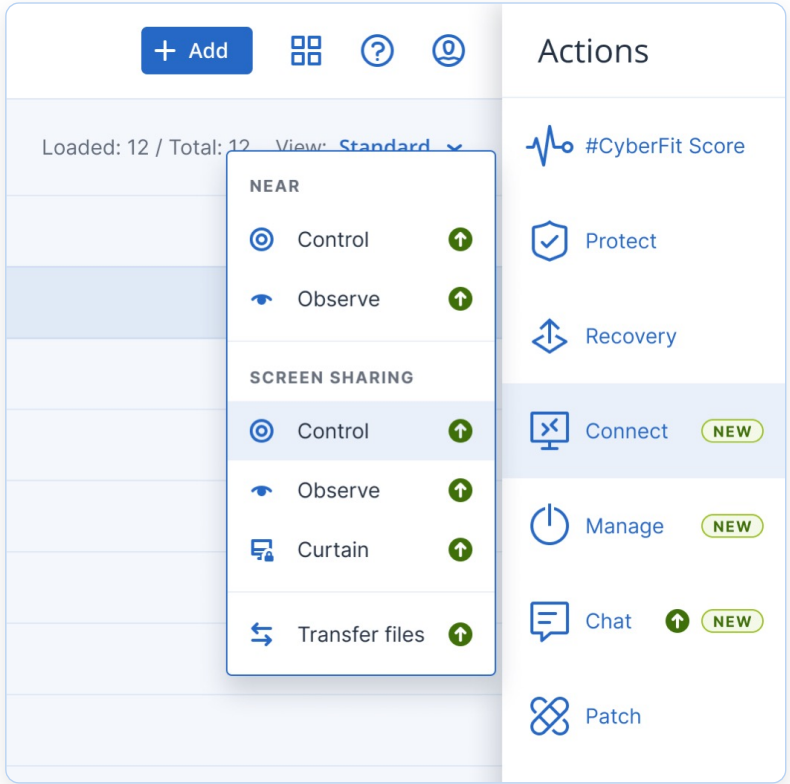
Escritorio remoto y asistencia a distancia

Escritorio remoto y asistencia a distancia

Es fácil de utilizar. Se trata de **una aplicación** que ofrece fácil acceso y soporte para equipos Windows, macOS y Linux, lo que ahorra el tiempo y el dinero que implica desplazarse in situ para aplicar la corrección, mediante el empleo de NEAR, un protocolo propio de Acronis de alta seguridad (en el que no se abren los puertos), totalmente integrado en Advanced Management y sin coste adicional.

La funcionalidad de escritorio remoto estándar se amplía con las siguientes funciones:

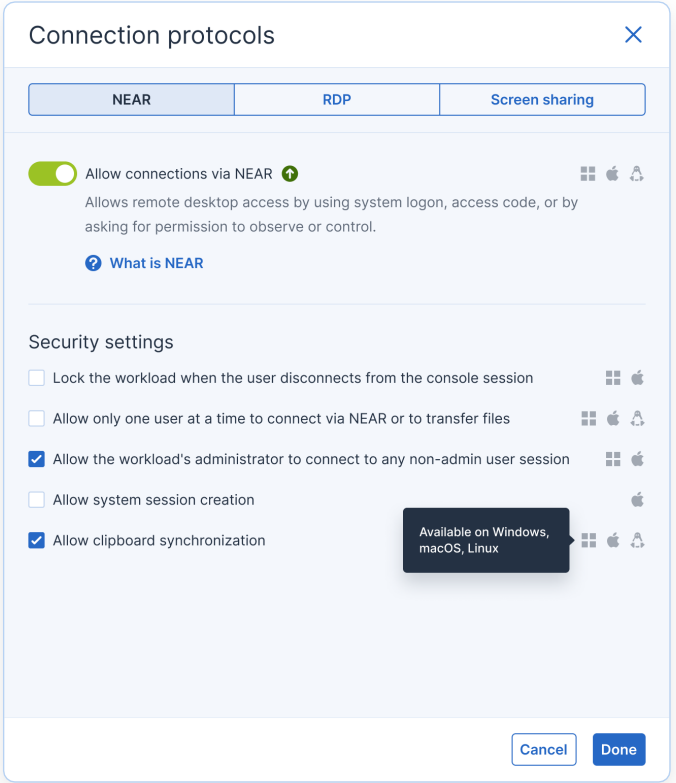
- Asistencia a distancia y control remoto para MacOS y Linux.
- Acceso remoto a través de NEAR y Apple Screen Sharing.
- Diferentes modos de conexión: Controlar, Observar y Cortina (solo para macOS).
- Conexiones remotas bajo demanda a equipos no gestionados a través de la aplicación Quick Assist.
- Transferencia de archivos entre equipos locales y remotos.
- Herramientas para administrar endpoint rápidamente: cierre, reinicio, suspensión, vaciar papelera, cerrar sesión.
- Grabación de sesiones (solo para conexiones NEAR).
- Informe sobre el historial de sesiones.
- Supervisión de equipos a distancia, a través de la transmisión de capturas de pantalla.



Escritorio remoto y asistencia a distancia

Ejemplo de casos de uso típicos con el escritorio remoto y la asistencia a distancia:

- Crear un plan de agente para habilitar las funcionalidades de escritorio remoto con protocolos de conexión.
- Conectarse a equipos Windows/macOS/Linux gestionados para prestar asistencia o resolver problemas a distancia.
- Transferir archivos entre equipos locales y remotos.
- Conectarse a equipos Windows/macOS descubiertos, a través de conexiones directas.
- Observar simultáneamente varios equipos remotos desde una sola ventana.
- Proporcionar soporte inmediato puntual a través de la aplicación Quick Assist.
- Cerrar, reiniciar, suspender, vaciar la papelera o cerrar la sesión en los equipos remotos.
- Grabar una sesión para fines de auditoría o para usarla como material de formación.
- Examinar un informe sobre todas las sesiones de escritorio remoto y de transferencia de archivos realizadas durante un período concreto.
- Supervisar el estado de los equipos a través de la transmisión de capturas de pantalla.



Acceso remoto rápido, estable y seguro

Acceda y administre equipos remotos de forma inmediata

Acceda a equipos remotos y resuelva problemas técnicos rápidamente, ahorrando el tiempo y el dinero que implica el desplazamiento para corregirlos in situ.

Aumente su eficiencia

Reduzca la pérdida de tiempo y proporcione soporte fiable con un excelente rendimiento, incluso en casos en los que se cuente con ancho de banda limitado.

Ofrezca asistencia remota segura

Garantice la seguridad de las conexiones con cifrado sofisticado, protección de datos de la cadena de claves y protección de la contraseña maestra para evitar el acceso no autorizado.

Las ventajas del escritorio remoto y la asistencia a distancia

Alto rendimiento

- Uso de aceleración de hardware de vídeo y audio pass-thru con baja latencia y compatibilidad con redes lentas.
- Reconexión automática cada vez que se produzca una interrupción en la red.

Seguridad

- Comunicación segura mediante cifrado AES bidireccional y el protocolo NEAR, exclusivo de Acronis. Ofrece compatibilidad multiplataforma (Windows, macOS, Linux), mayor rendimiento y seguridad reforzada en comparación con los métodos tradicionales, como el uso de RDP y puertos abiertos.
- Posibilidad de guardar las credenciales en un almacén seguro para realizar la autenticación automática en los equipos necesarios.

RDP, Apple Screen Sharing, Multiview

- Además de NEAR, Advanced Management admite conexiones de escritorio remoto a través del Protocolo de escritorio remoto (RDP) y Apple Screen Sharing.
- Visualización y cambio entre todos los escritorios remotos en una sola ventana.
- Posibilidad de realizar capturas de la pantalla remota, sin salir de la sesión remota.

Mayor compatibilidad

- Para todos los equipos Windows, macOS y Linux.
- Uso de ordenadores Windows, macOS y Linux como fuentes de conexión para el acceso remoto.
- Asistencia para el usuario dentro de la sesión y, por lo tanto, más eficaz.
- Transferencia de sesiones entre los técnicos.
- Conexión directa a equipos remotos mediante su dirección IP o su nombre DNS.

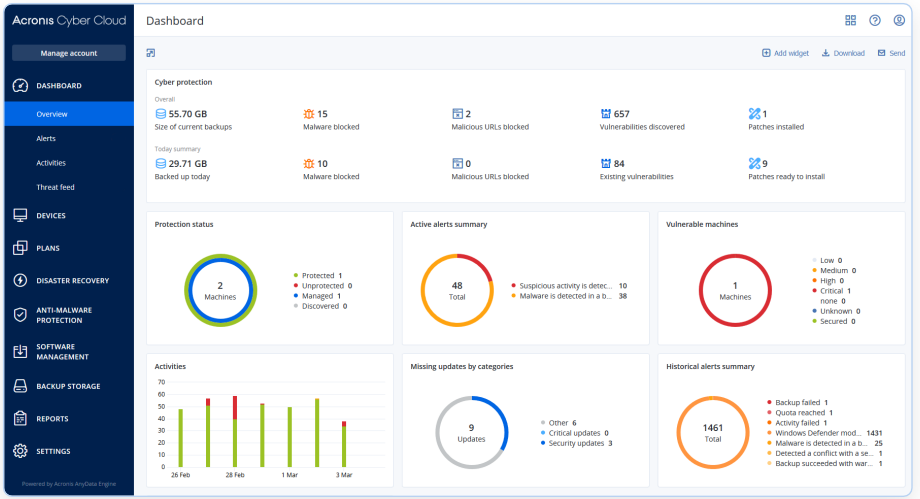
Acronis

Otras funciones de Acronis RMM

Programación y generación de informes con flexibilidad

Funciones avanzadas de generación de informes desde un solo panel:

- Control de las alertas activas
- Identificación de las actualizaciones que faltan
- Widgets personalizables en el panel
- Identificación rápida de los problemas
- Acceso rápido a acciones de administración
- Informes personalizables de resumen ejecutivo de clientes, para facilitar el inicio de una conversación con los clientes
- Planificación de informes
  - Para compartir internamente o con clientes
  - Utilice el formato que prefiera: XLS, PDF o CSV

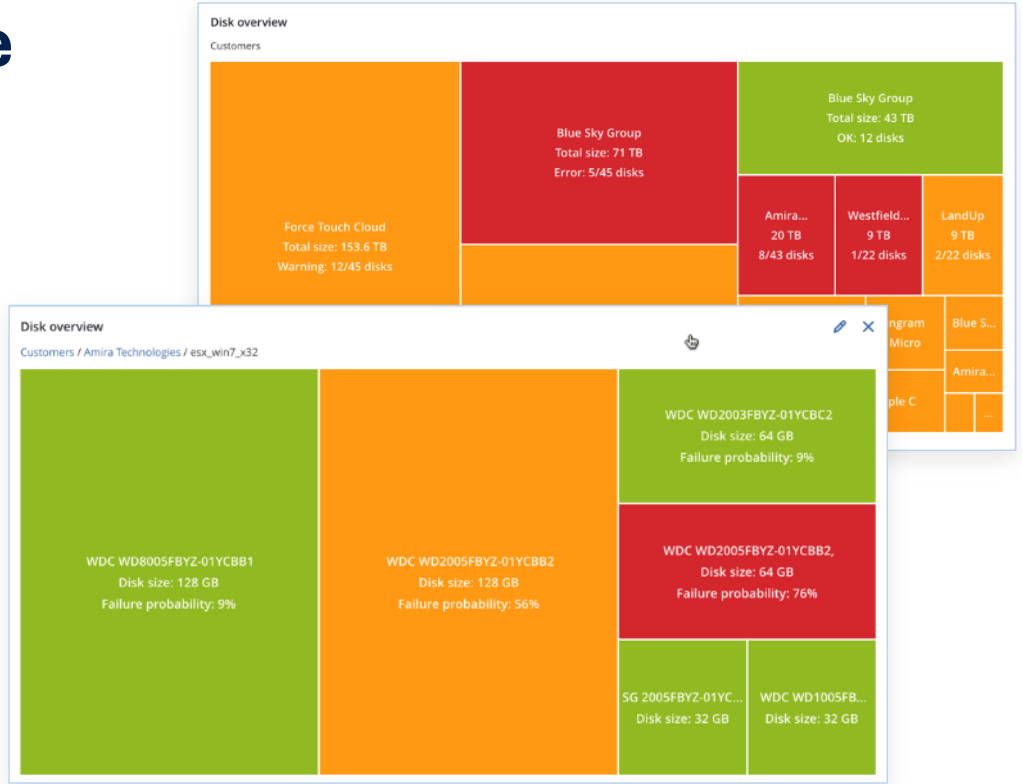


¿Por qué? Medio para demostrar el valor del MSP, agilizar las operaciones y simplificar las renovaciones.

Supervisión del estado de las unidades de disco

Identifique los problemas de discos antes de que fallen

- Utiliza una combinación de modelos de aprendizaje automático, informes S.M.A.R.T., tamaño y proveedor de la unidad, etc., para predecir fallos de discos HDD/SDD.
- Las predicciones son correctas en el **98,5 %** de los casos (y seguimos mejorando).
- Una vez que se genera una alerta, puede llevar a cabo la acción necesaria, por ejemplo, realizar una copia de seguridad de los archivos críticos que están en la unidad con errores.



¿Por qué? Prevención del tiempo de inactividad imprevisible o la pérdida de datos de clientes, planificación del trabajo de manera más eficaz, distinción de sus servicios.

Acronis

Acerca de Acronis

Acronis es líder en ciberseguridad y protección de datos para departamentos de TI

Suiza

Sede central en Schaffhausen, Suiza
Fundada en Singapur en 2003

En todo el mundo

Más de 1800 empleados en más de 50 países
Productos en 26 idiomas

Ciberseguridad

Más de 195 millones de amenazas y más de 61 millones de correos electrónicos maliciosos bloqueados en 2023

Más de 20.000

Partners
proveedores de servicios

Más de 750.000

Clientes
empresariales

54

Centros de datos
en todo el mundo