Acronis

Acronis Protected Workspace: protección del eslabón más débil

Los portátiles, los ordenadores de escritorio y las estaciones de trabajo son herramientas esenciales, pero también suponen un enorme riesgo de seguridad. Los empleados los utilizan en cualquier lugar, lo que los expone a una amplia gama de amenazas.

Para los proveedores de servicios gestionados (MSP), los dispositivos son los recursos más críticos y vulnerables que proteger. Sin embargo, no es tarea fácil, ya que los MSP suelen utilizar varias herramientas para proteger todos sus dispositivos. Y cuando estas herramientas no están integradas de forma nativa, lograr que funcionen juntas puede ser difícil y generar brechas en la cobertura.

Además, la gestión de varias herramientas implica el uso de interfaces diferentes, lo que aumenta la complejidad, introduce riesgos y a menudo requiere conocimientos especializados. En última instancia, las infraestructuras de seguridad de los espacios de trabajo, construidas a partir de múltiples herramientas, aumentan los costes operativos, generan ineficiencias y disminuyen la protección global.

Con los ciberdelincuentes utilizando la IA para crear variantes de ataque casi infinitas, prácticamente todos los días estamos expuestos a ataques de día cero. El riesgo es considerable: los ataques exitosos provocan tiempos de inactividad, pérdida de productividad y daños a la reputación tanto para los MSP como para sus clientes, además de generar problemas de cumplimiento normativo en numerosos sectores.

Protección de datos, administración de endpoints y seguridad integradas de forma nativa para espacios de trabajo

Desafíos empresariales a los que se enfrentan los MSP para proteger espacios de trabajo

Muchas organizaciones no cuentan con los recursos necesarios para gestionar la seguridad de sus espacios de trabajo y recurren a los MSP en busca de ayuda. Necesitan que los proveedores de servicios protejan todos los portátiles y ordenadores de escritorio, independientemente de donde se ubiquen, de tal forma que se protejan los datos sin sacrificar la productividad.

El ritmo y la naturaleza global de las operaciones empresariales hacen que esa tarea resulte difícil para los proveedores de servicios. Parte del problema es la escalabilidad. Cientos o miles de dispositivos crean una amplia superficie de ataque que los MSP deben proteger. Un único endpoint comprometido puede dar lugar a un ciberataque que paralice por completo las operaciones del cliente.

Los clientes también suelen tener empleados que utilizan dispositivos en distintas ubicaciones y envían datos por todo el mundo. El teletrabajo añade complejidad a la protección de los espacios de trabajo. La movilidad de los dispositivos, las operaciones globales y las expectativas de respuestas rápidas dejan los dispositivos de los empleados totalmente expuestos a los ciberataques. Y en sectores como la sanidad y las finanzas, unos espacios de trabajo mal protegidos pueden poner en riesgo el cumplimiento normativo.

El desafío de la seguridad de los espacios de trabajo para los MSP

Proteger los espacios de trabajo resulta todo un desafío para los MSP, ya que las herramientas de ciberseguridad destinadas a garantizar la seguridad de los dispositivos no ofrecen la eficacia que necesitan los proveedores de servicios. Las herramientas fragmentadas, con el antivirus en una aplicación, las copias de seguridad en otra y la Administración y supervisión remotas (RMM) en otra distinta, hacen que la protección de los espacios de trabajo sea costosa y propensa a errores.

Cada elemento de protección requiere una aplicación y una configuración únicas; el número de combinaciones entre dispositivos es prácticamente ilimitado. En estos casos, los MSP necesitan mucho más personal para gestionarlo todo. O bien deben contratar a varios técnicos, o dedicar tiempo a formar a sus técnicos para que utilicen varias aplicaciones independientes y confiar en que lo hagan todo bien.

Gestionar diferentes herramientas en múltiples consolas provoca tiempos de respuesta lentos, así como agotamiento y errores por parte de los técnicos. Además, deja abierta la posibilidad de que se realicen integraciones incorrectas que pueden generar enormes brechas de seguridad.

Los espacios de trabajo rara vez están "apagados", por lo que son un objetivo constante de los ciberataques. Además, los empleados de los clientes suelen confiar demasiado en sus dispositivos, lo que crea una capa de vulnerabilidad adicional. Los MSP necesitan una solución para proteger los espacios de trabajo que ofrezca funciones de seguridad integrales y que, sobre todo, sea fácil de gestionar.

"Muchas organizaciones cuentan con una infraestructura de seguridad fragmentada en sus espacios de trabajo, lo que ha provocado un aumento en los costes operativos, mayor complejidad y una menor eficacia en la protección".

Gartner: Hoja de ruta estratégica para la seguridad de espacios de trabajo (2025)

Acronis Protected Workspace ofrece servicios adaptados a los MSP

Acronis Protected Workspace incluye una serie de servicios integrados de forma nativa que permiten a los MSP proteger los dispositivos de sus clientes con un riesgo mínimo y con la máxima eficacia. Están disponibles por carga de trabajo o por gigabyte e incluyen lo siguiente:

Servicios en Acronis Protected Workspace

Acronis Backup para estaciones de trabajo	Almacena y protege los datos de los portátiles, ordenadores de escritorio y estaciones de trabajo de los clientes.
Acronis Advanced Backup para estaciones de trabajo	Amplía las funciones de copia de seguridad de la nube para proteger de forma proactiva los datos de los espacios de trabajo de los clientes en más de 20 tipos de cargas de trabajo, lo que elimina prácticamente los tiempos de inactividad.
Acronis Endpoint Detection and Response (EDR)	Supervisa activamente los endpoints, detiene los ataques antes de que puedan causar daños y ofrece recuperación con un solo clic.
Acronis Extended Detection and Response (XDR)	Ofrece una protección activa completa, diseñada para prevenir, detectar y analizar incidentes, así como para responder ante ellos y recuperar los sistemas y datos afectados.
Acronis Remote Monitoring and Management (RMM)	Servicios superiores de administración y supervisión, con un enfoque centrado en la seguridad. Automatícelo todo y acelere los procesos gracias a la IA y el aprendizaje automático, junto con un potente motor de scripting. Descubra y proteja los espacios de trabajo conectados con Device Sense™.
Acronis Data Loss Prevention (DLP)	Evita las fugas de datos desde los endpoints sin necesidad de instalaciones complejas ni de conocimientos especializados en privacidad.
Acronis Active Protection	Protege activamente todos los datos de los sistemas de los clientes, incluidos documentos, archivos multimedia y programas entre otros.
Acronis Antimalware	Protege los sistemas de los clientes, en tiempo real y de forma proactiva, frente a los ciberataques avanzados, con tecnologías antivirus, antimalware y antiransomware, basadas en IA y en heurística estática y de comportamientos.

Los MSP también tienen la opción de elegir paquetes basados en soluciones, incluidos los siguientes:

Workstation Backup	Endpoint Security + RMM	Ultimate Protection
Copia de seguridad de Acronis para estaciones de trabajo con 300 GB de almacenamiento incluidos	Acronis Active Protection	Paquete de seguridad+ RMM
	Acronis Antimalware	Paquete de copia de seguridad + almacenamiento en la nube
	Acronis EDR	Acronis Advanced Backup
	Acronis XDR	Acronis DLP
	Acronis RMM	

El potencial de una protección de espacios de trabajo integrada de forma nativa

Los MSP necesitan un método unificado, eficaz y rentable de proteger, gestionar y recuperar los espacios de trabajo. Acronis Protected Workspace ofrece a los MSP todos los servicios que necesitan para proteger los espacios de trabajo en una única solución integrada de forma nativa: un solo agente, una licencia y una única consola para administrarlo todo. Se trata de una idea sencilla pero potente que permite a los técnicos gestionar más espacios de trabajo con mayor seguridad.

Acronis Protected Workspace también ofrece:

- **Integración nativa** con seguridad para endpoints, RMM y copias de seguridad en una única consola.
- **Protección integral:** antimalware con IA, Detección y respuesta para endpoints (EDR), Detección y respuesta ampliadas (XDR), detección de ransomware y análisis de comportamientos alineados con el marco de ciberseguridad del NIST.
- **Eficacia operativa:** resolución más rápida de las incidencias, mejor servicio a los clientes y menores costes de formación.
- **Flexibilidad:** modelos de licencia adaptados a los MSP, con la posibilidad de crear paquetes de protección personalizados.

"Acronis, como nuestra plataforma principal, lo abarca todo. La eficacia que aporta es inigualable: nos permite ahorrar tiempo, reducir costes y minimizar los esfuerzos de formación. Tenerlo todo en una única consola facilita y simplifica la administración de nuestra oferta de servicios".

– Joshua Aaronson, cofundador de Panda Technology

Acronis Protected Workspace ofrece todo lo que necesitan los MSP para proteger dispositivos

Con Acronis Protected Workspace, los MSP pueden afrontar el desafío de proteger portátiles, ordenadores de escritorio y estaciones de trabajo sin tener que lidiar con la gestión de múltiples aplicaciones de seguridad independientes. Los proveedores de servicios pueden diferenciarse de la competencia al ofrecer una mejor protección, tiempos de respuesta más rápidos y un servicio de atención al cliente superior.

Vea Acronis Protected Workspace en acción CONTÁCTENOS

Acronis

Obtenga más información en www.acronis.com