Habilitación de Endpoint Protection

Los sistemas informáticos que interactúan directamente con los usuarios se consideran sistemas de punto de conexión. Los sistemas de los dispositivos, como portátiles, smartphones, tabletas y equipos, deben protegerse para evitar que actúen como puertas de enlace para ataques de seguridad en los sistemas conectados en red de una organización.

Anteriormente, analizamos las responsabilidades compartidas para ayudar a proteger los servicios en Azure. IaaS implica más responsabilidad del cliente que PaaS y SaaS, y Microsoft Defender for Cloud proporciona las herramientas necesarias para proteger la red, ayudar a proteger los servicios y mantenerse al día en la posición de seguridad.

Primer paso: ayudar a proteger contra malware

Instale antimalware para ayudar a identificar y quitar virus, spyware y otro software malintencionado. Puede instalar Microsoft Antimalware o una solución de Endpoint Protection de un partner de Microsoft.

Segundo paso: supervisar el estado del antimalware

A continuación, integre la solución antimalware con Microsoft Defender for Cloud para supervisar el estado de la protección antimalware. Security Center informa de esto en la hoja **Incidencias de Endpoint Protection**. Security Center resalta las incidencias, como las amenazas detectadas y si la protección es insuficiente, lo cual puede hacer vulnerables sus equipos y máquinas virtuales frente a amenazas de malware. Si usa la información descrita en Incidencias de Endpoint Protection, puede preparar un plan para solucionar cualquier incidencia detectada.

Al centrarse solo en la recomendación del punto de conexión, ¿qué notifica Microsoft Defender for Cloud como problemas?

Si aplica la información descrita en **Incidencias de Endpoint Protection**, puede identificar un plan para solucionar cualquier incidencia detectada.

Security Center notifica las siguientes incidencias de Endpoint Protection:

- **Endpoint Protection no está instalado en las máquinas virtuales de Azure**: no hay ninguna solución antimalware compatible instalada en estas máquinas virtuales de Azure.
- **Endpoint Protection no instalado en los equipos que no son de Azure**: no hay ningún antimalware compatible instalado en estos equipos que no son de Azure.
- Incidencias de estado de Endpoint Protection:
    - **Firma sin actualizar**. Hay una solución antimalware instalada en estos equipos y máquinas virtuales, pero no cuenta con las firmas de antimalware más recientes.
    - **Sin protección en tiempo real**. Hay una solución antimalware instalada en estos equipos y máquinas virtuales, pero no está configurada para la protección en

tiempo real. El servicio podría deshabilitarse o es posible que Security Center no pueda obtener el estado, ya que la solución no es compatible.

- **Sin generación de informes**. Hay una solución antimalware instalada, pero no notifica datos.
- **Desconocido**. Hay una solución antimalware instalada, pero su estado es desconocido o informa de un error desconocido.
