¿Qué preguntas debemos hacerle a cualquier proveedor de seguridad para endpoints?

Respuesta breve: Pregunte dónde se toman las decisiones, qué ocurre sin conectividad, de qué depende la herramienta para funcionar y si previene o simplemente informa. Las respuestas separan rápidamente la arquitectura del marketing.

Preguntas que vale la pena hacer

1. **¿Dónde se toma la decisión de protección: en el endpoint o en su nube?** Un intercambio de red en la ruta crítica no puede superar a un ataque de escala de milisegundos.
2. **¿Qué ocurre cuando el equipo está fuera de línea o aislado (air-gapped)?** Si la protección se degrada, no era local.
3. **¿Su agente depende de las bibliotecas del sistema de Windows para funcionar?** Si es así, un atacante que comprometa esas bibliotecas en memoria puede cegarlo o silenciarlo.
4. **¿Requieren firmas o fuentes de inteligencia de amenazas?** Si es así, la protección va, por definición, un paso detrás del atacante.
5. **¿Una respuesta requiere intervención humana?** Si es así, el tiempo de respuesta está limitado por la biología humana.
6. **¿Almacenan nuestras claves de cifrado o cargan datos sensibles para su análisis?** El almacenamiento centralizado crea un objetivo y un riesgo de divulgación forzada.
7. **¿Cuál es su tasa de falsos positivos, y qué hace realmente una respuesta?** El bloqueo total del sistema como única opción de contención resulta costoso en un hospital o una planta industrial.

Por qué importan estas preguntas

La mayoría de las herramientas para endpoints se ven similares en una ficha técnica. Estas preguntas ponen de manifiesto las decisiones arquitectónicas que determinan si una herramienta puede actuar a tiempo, o si solo puede explicar, después del hecho, lo que ocurrió.

Revision #1
Created 2026-07-24 01:54:10 UTC by Dennis Underwood

Updated 2026-07-24 01:54:10 UTC by Dennis Underwood