What questions should we ask any endpoint security vendor?

Short answer: Ask where decisions are made, what happens without connectivity, what the tool depends on to function, and whether it prevents or merely reports. The answers separate architecture from marketing quickly.

Questions worth asking

1. **Where is the protective decision made — on the endpoint or in your cloud?** A network round trip in the critical path cannot beat a millisecond-scale attack.
2. **What happens when the machine is offline or air-gapped?** If protection degrades, it wasn't local.
3. **Does your agent depend on Windows system libraries to function?** If yes, an attacker who compromises those libraries in memory can blind or silence it.
4. **Do you require signatures or threat intelligence feeds?** If yes, protection trails the attacker by definition.
5. **Does a response require a human?** If yes, response time is bounded by human biology.
6. **Do you store our encryption keys or upload sensitive data for analysis?** Centralized storage creates a target and a compelled-disclosure risk.
7. **What is your false positive rate, and what does a response actually do?** Full-system lockdown as the only containment option is expensive in a hospital or a plant.

Why these questions matter

Most endpoint tools look similar in a datasheet. These questions surface the architectural decisions that determine whether a tool can act in time — or can only explain, afterward, what happened.

Revision #3
Created 2026-07-20 19:24:18 UTC by Dennis Underwood
Updated 2026-07-21 19:32:32 UTC by Dennis Underwood