Que perguntas devemos fazer a qualquer fornecedor de segurança de endpoint?

Resposta curta: Pergunte onde as decisões são tomadas, o que acontece sem conectividade, do que a ferramenta depende para funcionar e se ela previne ou apenas reporta. As respostas separam rapidamente a arquitetura do marketing.

Perguntas que vale a pena fazer

1. **Onde é tomada a decisão de proteção — no endpoint ou na sua nuvem?** Uma ida e volta pela rede no caminho crítico não pode superar um ataque em escala de milissegundos.
2. **O que acontece quando a máquina está offline ou isolada da rede (air-gapped)?** Se a proteção se degrada, ela não era local.
3. **O seu agente depende de bibliotecas do sistema Windows para funcionar?** Se sim, um atacante que comprometa essas bibliotecas em memória pode cegá-lo ou silenciá-lo.
4. **Vocês exigem assinaturas ou feeds de inteligência de ameaças?** Se sim, a proteção fica atrás do atacante por definição.
5. **Uma resposta requer intervenção humana?** Se sim, o tempo de resposta é limitado pela biologia humana.
6. **Vocês armazenam nossas chaves de criptografia ou enviam dados sensíveis para análise?** O armazenamento centralizado cria um alvo e um risco de divulgação compulsória.
7. **Qual é a sua taxa de falsos positivos, e o que uma resposta realmente faz?** O bloqueio total do sistema como única opção de contenção é dispendioso em um hospital ou em uma fábrica.

Por que essas perguntas importam

A maioria das ferramentas de endpoint parece semelhante em uma ficha técnica. Essas perguntas revelam as decisões arquitetônicas que determinam se uma ferramenta consegue agir a tempo — ou se só consegue explicar, depois, o que aconteceu.

Revision #1
Created 2026-07-24 05:52:41 UTC by Dennis Underwood

Updated 2026-07-24 05:52:41 UTC by Dennis Underwood