

Quelles questions devrions-nous poser à tout fournisseur de sécurité des terminaux ?

Réponse courte : Demandez où les décisions sont prises, ce qui se passe en l'absence de connectivité, de quoi l'outil dépend pour fonctionner, et s'il prévient ou se contente de signaler. Les réponses permettent de distinguer rapidement l'architecture du marketing.

Questions qu'il vaut la peine de poser

1. **Où la décision de protection est-elle prise — sur le terminal ou dans votre cloud ?** Un aller-retour réseau dans le chemin critique ne peut pas rivaliser avec une attaque se déroulant à l'échelle de la milliseconde.
2. **Que se passe-t-il lorsque la machine est hors ligne ou isolée du réseau (air-gapped) ?** Si la protection se dégrade, ce n'est pas qu'elle était locale.
3. **Votre agent dépend-il des bibliothèques système Windows pour fonctionner ?** Si oui, un attaquant qui compromet ces bibliothèques en mémoire peut l'aveugler ou le réduire au silence.
4. **Exigez-vous des signatures ou des flux de renseignement sur les menaces ?** Si oui, la protection est par définition à la traîne par rapport à l'attaquant.
5. **Une réponse nécessite-t-elle une intervention humaine ?** Si oui, le temps de réponse est limité par la biologie humaine.
6. **Stockez-vous nos clés de chiffrement ou téléversez-vous des données sensibles à des fins d'analyse ?** Un stockage centralisé crée une cible et un risque de divulgation forcée.
7. **Quel est votre taux de faux positifs, et que fait réellement une réponse ?** Le verrouillage complet du système comme seule option de confinement est coûteux dans un hôpital ou une usine.

Pourquoi ces questions sont importantes

La plupart des outils de sécurité des terminaux se ressemblent sur une fiche technique. Ces questions font apparaître les décisions architecturales qui déterminent si un outil peut agir à temps — ou s'il peut seulement expliquer, après coup, ce qui s'est passé.

Revision #1

Created 2026-07-24 07:03:26 UTC by Dennis Underwood

Updated 2026-07-24 07:03:26 UTC by Dennis Underwood