

Welche Fragen sollten wir jedem Anbieter von Endpunktsicherheit stellen?

Kurze Antwort: Fragen Sie, wo Entscheidungen getroffen werden, was ohne Konnektivität passiert, wovon das Tool zur Funktion abhängig ist, und ob es verhindert oder lediglich meldet. Die Antworten trennen Architektur schnell von Marketing.

Fragen, die es sich zu stellen lohnt

1. **Wo wird die schützende Entscheidung getroffen — auf dem Endpunkt oder in Ihrer Cloud?** Ein Netzwerk-Roundtrip im kritischen Pfad kann einen Angriff im Millisekundenbereich nicht schlagen.
2. **Was passiert, wenn das Gerät offline oder air-gapped ist?** Wenn der Schutz nachlässt, war er nicht lokal.
3. **Ist Ihr Agent zur Funktion auf Windows-Systembibliotheken angewiesen?** Falls ja, kann ein Angreifer, der diese Bibliotheken im Arbeitsspeicher kompromittiert, ihn blenden oder zum Schweigen bringen.
4. **Benötigen Sie Signaturen oder Threat-Intelligence-Feeds?** Falls ja, hinkt der Schutz dem Angreifer per Definition hinterher.
5. **Erfordert eine Reaktion einen Menschen?** Falls ja, ist die Reaktionszeit durch die menschliche Biologie begrenzt.
6. **Speichern Sie unsere Verschlüsselungsschlüssel oder laden Sie sensible Daten zur Analyse hoch?** Zentralisierte Speicherung schafft ein Ziel und ein Risiko der erzwungenen Offenlegung.
7. **Wie hoch ist Ihre Falsch-Positiv-Rate, und was bewirkt eine Reaktion tatsächlich?** Eine vollständige Systemspernung als einzige Eindämmungsoption ist in einem Krankenhaus oder einer Anlage kostspielig.

Warum diese Fragen wichtig sind

Die meisten Endpunkt-Tools wirken in einem Datenblatt ähnlich. Diese Fragen bringen die architektonischen Entscheidungen zutage, die darüber bestimmen, ob ein Tool rechtzeitig handeln kann — oder nur im Nachhinein erklären kann, was geschehen ist.

