

Qu'est-il advenu du modèle du « collecteur passif » de l'industrie de la sécurité ?

Réponse courte : Pendant des années, les éditeurs ont affirmé que le traitement local sur le point de terminaison était obsolète et ont mis en avant des agents légers qui transmettent la télémétrie brute vers des solutions d'analyse dans le cloud. Les attaques modernes en mémoire visant les bibliothèques centrales du système d'exploitation ont mis ce modèle en échec — les agents continuent de fonctionner mais deviennent en réalité aveugles et muets.

Pourquoi ce modèle a été adopté

Il était moins coûteux à mettre en œuvre. L'ingénierie au niveau du noyau est difficile et onéreuse ; l'envoi de la télémétrie vers le cloud permettait aux éditeurs de proposer des logiciels de point de terminaison peu coûteux, de monétiser de vastes réserves de stockage cloud et de mettre en avant leurs capacités d'IA cloud. Le modèle était optimisé pour l'économie du développement, non pour la défense.

Pourquoi ce modèle échoue aujourd'hui

Ces agents dépendent entièrement des composants natifs du système d'exploitation pour fonctionner et collecter des données. Lorsque les attaquants compromettent ces composants en mémoire, l'agent ne plante pas — il continue de fonctionner mais ne signale plus rien, laissant un tableau de bord indiquant que tout va bien alors que des données sont exfiltrées.

Il existe également des cas documentés d'interdiction délibérée : des attaquants, et dans certains cas vérifiés des concurrents cherchant à dissimuler leurs propres failles, exploitent activement ces dépendances de bibliothèques pour forcer l'arrêt ou saboter les défenses des points de terminaison.

L'impasse architecturale

Corriger ce problème exigerait des éditeurs historiques qu'ils abandonnent leurs pipelines de télémétrie axés sur le cloud et reconstruisent leurs solutions autour d'une informatique en périphérie locale, au niveau du noyau — un effort s'étalant sur plusieurs années. Les acquisitions

récentes et les investissements en capital-risque montrent au contraire que l'industrie s'oriente davantage vers l'analyse dans le cloud et les lacs de données centralisés.

Revision #1

Created 2026-07-24 07:03:37 UTC by Dennis Underwood

Updated 2026-07-24 07:03:37 UTC by Dennis Underwood