O que aconteceu com o modelo de "coletor burro" do setor de segurança?

Resposta curta: Durante anos, os fornecedores recomendaram que o processamento local no endpoint estava obsoleto e promoveram agentes leves que encaminham telemetria bruta para análises em nuvem. Ataques modernos em memória contra bibliotecas centrais do sistema operacional expuseram esse modelo — os agentes continuam em execução, mas ficam efetivamente cegos e mudos.

Por que o modelo foi adotado

Era mais barato de construir. A engenharia em nível de kernel é difícil e cara; enviar telemetria para a nuvem permitiu que os fornecedores lançassem software de endpoint de baixo custo, monetizassem grandes pools de armazenamento em nuvem e comercializassem capacidades de IA em nuvem. O modelo foi otimizado para a economia de desenvolvimento, não para a defesa.

Por que está falhando agora

Esses agentes dependem inteiramente de componentes nativos do sistema operacional para funcionar e coletar dados. Quando os invasores comprometem esses componentes em memória, o agente não trava — ele continua em execução e não relata nada, deixando um painel que indica que está tudo bem enquanto os dados são exfiltrados.

Há também interdição deliberada documentada: invasores, e em alguns casos verificados concorrentes que buscam mascarar suas próprias falhas, exploram ativamente essas dependências de bibliotecas para forçar o encerramento ou sabotar as defesas de endpoint.

O beco sem saída arquitetônico

Corrigir isso exigiria que os fornecedores tradicionais abandonassem os pipelines de telemetria voltados para a nuvem e reconstruíssem para computação de borda local, em nível de kernel — um esforço de vários anos. Aquisições recentes e investimentos de capital de risco mostram o setor avançando ainda mais em direção a análises em nuvem e data lakes centralizados, em vez disso.

Revision #1
Created 2026-07-24 05:52:50 UTC by Dennis Underwood
Updated 2026-07-24 05:52:51 UTC by Dennis Underwood