O que significa neutralidade geopolítica em software de segurança?

Resposta curta: Significa que o software é construído para proteger a sua organização sem incorporar backdoors estratégicos estrangeiros, parcerias de inteligência com estados estrangeiros ou dependências obrigatórias de nuvem — de modo que a sua utilização não importe os interesses estratégicos de outro país para a sua infraestrutura.

O problema que aborda

As ferramentas de segurança legadas frequentemente dependem de modelos centralizados de recolha em nuvem que exfiltram continuamente telemetria de endpoints, detalhes de contas e artefactos do sistema de ficheiros através de fronteiras nacionais e geopolíticas. Isso é lento face a ataques à velocidade das máquinas e cria exposição de conformidade e segurança ao abrigo do GDPR, da Saudi PDPL, da Lei Federal por Decreto n.º 45/2021 dos EAU e da Lei de Proteção de Dados do Quénia.

Também cria uma questão que a maioria dos processos de aquisição nunca coloca: *em que jurisdição acaba a minha telemetria, e quem mais lhe consegue aceder aí?*

Os três componentes

1. **Ausência de backdoors estratégicos estrangeiros** — sem componentes de código patrocinados por estados nem SDKs estrangeiros não verificados.
2. **Ausência de parcerias de inteligência com estados estrangeiros** — a telemetria do cliente não é partilhada com terceiros, incluindo governos.
3. **Ausência de dependência obrigatória de nuvem** — o software funciona totalmente offline, pelo que nenhum dado precisa de atravessar uma fronteira para que o produto funcione.

O terceiro ponto é o que torna os dois primeiros aplicáveis. Um produto que *exige* uma ligação à nuvem não pode prometer de forma credível que os seus dados permanecem no local.

Revision #1
Created 2026-07-24 05:54:36 UTC by Dennis Underwood
Updated 2026-07-24 05:54:36 UTC by Dennis Underwood