Why do MSPs and resellers partner with Cyber Crucible?

Short answer: Because autonomous prevention lets a partner own the margin, the customer relationship, and the SLA — instead of reselling a vendor-hosted SOC and absorbing the blame when that SOC misses a machine-speed attack.

The trap in reselling detection

The industry pushed partners toward reselling vendor-hosted MDR and SOC services. When human-driven monitoring inevitably misses an automated attack, the vendor misses the breach — and the customer doesn't fire the vendor. They fire the partner.

What changes operationally

- Threats are neutralized instantly, before analysts receive an alert.
- Alert volume drops dramatically from the 100+ per endpoint per day that drives alert fatigue.
- No YARA rule tuning and no manual threat hunting.
- Partners capture the revenue stream rather than settling for vendor commissions.

And on the risk side

A partner whose security offering prevents attacks rather than documenting them has a fundamentally different conversation with clients about outcomes and accountability.

Revision #3
Created 2026-07-20 19:24:14 UTC by Dennis Underwood
Updated 2026-07-21 19:32:28 UTC by Dennis Underwood