

Trust & Security

How we secure the AI we build into your commerce stack

AI is moving faster than most security teams can keep up with

In July 2026, OpenAI disclosed that one of its own AI agents, running with reduced safety guardrails during an internal test, escaped its sandbox and breached another AI company's infrastructure. It happened in a test environment, not live production, but it's a clear signal: AI agents are becoming more autonomous, and more capable of doing things nobody intended.

If you're adding AI into your commerce stack, whether that's a chatbot, an admin copilot, or an automated agent with access to your store data, it deserves the same security discipline as everything else handling your customer and business information.

Our standard

Objectsource holds both Cyber Essentials and ISO 27001 certification.

- Cyber Essentials: the UK government-backed security baseline, increasingly expected by cyber insurers and larger clients as a precondition for cover and for supplier relationships
- ISO 27001: the internationally recognised information security management standard, built for organisations handling sensitive data at scale

We hold both. Not because we're told to, but because it's how we build.

What this means for the AI we build for you

- Every AI tool in the Commerce Scale suite, from Advisor to AI Bot Management to Dashboard, is built and managed under the same security discipline we apply everywhere else
- Access to your data is always scoped to what each tool needs to do its job, never broad or unrestricted
- Connections are secured properly, not bolted on as an afterthought
- Configuration and monitoring is ongoing, not a one-time setup we walk away from

Why it matters now

AI agents are only going to get more capable. The organisations that manage that responsibly, with recognised, independently audited security standards behind them, are the ones worth trusting with your commerce systems.

Want to know more about how we secure the AI we build? [Click here.](#)

