

Make safe AI adoption your next managed service

Barracuda® AI Data Security helps MSPs uncover shadow AI, guide safe AI adoption, and build recurring AI governance services across every customer.

Generative AI (GenAI) didn't arrive through the front door. It arrived on your customers' phones and browsers, one employee at a time, long before anyone wrote a policy. The productivity is real. So is the exposure: staff paste customer records, source code and contracts into tools no one has vetted.

Your customers know they can't ban AI, and they don't want to. What they lack is a way to say yes with confidence. That gap is your opening. With Barracuda AI Data Security, you can walk in with a plan, show them exactly what's happening in their environment, and build a managed practice around safe adoption, one that moves them up an AI governance maturity model from ad hoc use to a managed, monitored posture. It's a consultative motion that makes you harder to replace and easier to renew.

Stat band

69%

of organizations have evidence employees use prohibited public GenAI tools

Gartner, 2025

37%

Have policies to manage AI or detect Shadow AI

IBM Cost of a Data Breach, 2025

+\$670K

Added to the average breach cost where Shadow AI is high

IBM Cost of a Data Breach, 2025

Play 1 — Open with a policy, not a pitch

The play

Most of your customers have no written rules for AI at all. Lead with something immediately useful: the Barracuda AI Acceptable Use Policy template, a customizable framework aligned to the NIST AI Risk Management Framework and ISO/IEC 42001, covering approved tools, data classification, AI agents, and incident response. In a single meeting you move the customer from “should we be worried about AI?” to “here’s your policy, now let’s put it to work.”

Why it grows your business

The template costs you nothing to hand over and it immediately positions you as the advisor, not the vendor. It also plants the question every customer asks next: “How do we know anyone’s actually following this?” That question is precisely the service you sell in the next three plays.

Play 2 — Expose the invisible

The play

You can’t govern what you can’t see. Barracuda AI Data Security discovers the GenAI tools employees are already using, sanctioned or not, and automatically classifies each service by risk. Run it as a complimentary discovery exercise for an existing customer and you turn “we think some people use ChatGPT” into a named, ranked inventory of real exposure.

Why it grows your business

Discovery hands you a concrete, undeniable finding to bring back to the customer and that’s the moment a wait-and-see conversation becomes a buying decision. It’s repeatable across your entire base, and it’s the evidence that justifies a managed service instead of a one-off project.

Play 3 — Let the reports do the talking

The play

Raw discovery data doesn’t move a customer, but a picture does. Built-in reports translate the findings into something a business owner understands at a glance: which AI tools are in use, how risky each one is, and where sensitive data is heading. You walk into the room with a report that makes the invisible impossible to ignore, then use it to prioritize what to govern first.

Why it grows your business

The report is your recurring touchpoint. Drop it into every QBR and you have a standing reason to be in front of the customer, a visible record of the risk you’re retiring and a natural bridge to the next tier of protection, without ever sounding like you’re upselling.

Play 4 — Turn it into a service, not a project

The play

Policy, discovery, and reporting aren't one-time deliverables — they're a cycle. Adoption changes monthly, new tools appear, and the policy must keep pace. Package it as an ongoing AI governance service where you monitor usage, refresh the report each quarter, tune the policy, and add guardrails that warn on or block risky data sharing as the customer matures. Barracuda AI Data Security gives you the tooling to run this at scale across your whole book of business.

Why it grows your business

This is the point of the whole motion. A governance service is recurring revenue, not a one-off invoice. It's sticky because you're woven into how the customer operates, and it's a genuine differentiator against break-fix competitors still pretending AI isn't happening. You stop being a line item and become the advisor they call first.

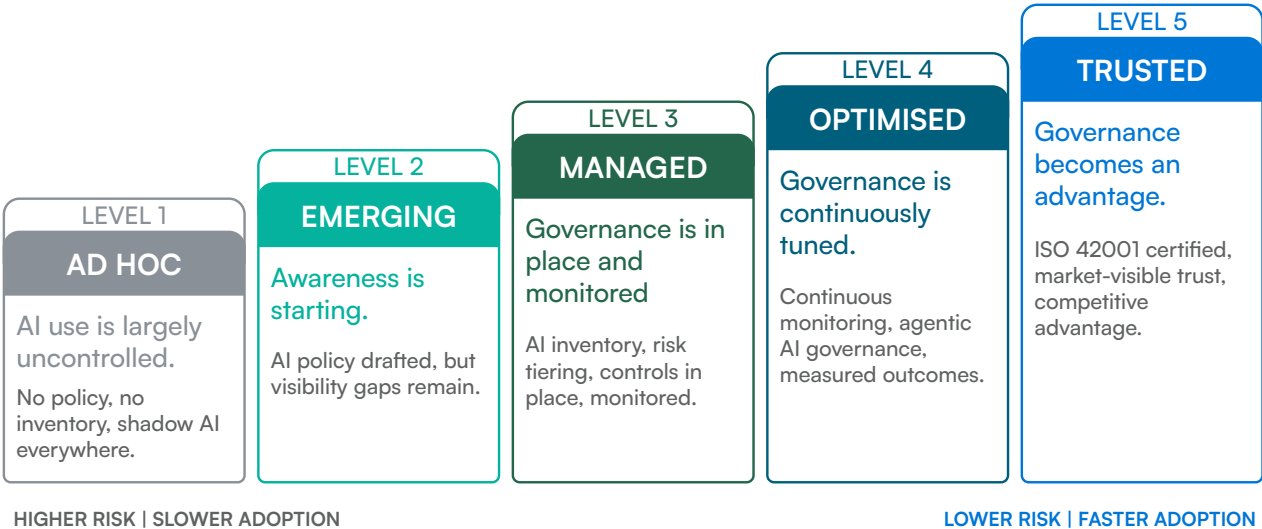
The AI Governance Maturity Model

Kicker

Aligned to the NIST AI Risk Management Framework and ISO/IEC 42001

AI governance maturity measures how effectively an organization can discover AI use, assess risk, apply governance controls, and demonstrate compliance. Higher levels of AI governance maturity make it easier to adopt AI safely, satisfy governance requirements, and reduce business risk. The five AI governance maturity levels are Ad Hoc, Emerging, Managed, Optimized, and Trusted.

A simple, shared reference for AI governance maturity — the same five-stage progression organizations already use for cyber, data, and cloud. It runs from ad hoc, unmanaged AI use through a governed, monitored posture, and on to the Optimized and Trusted stages that mark a fully mature program — a common language you and your customers can plan against.



Risk decreases as visibility, control and evidence increase, while confidence in AI adoption improves.

Getting started in three steps

STEP 1

Pick a customer and run discovery

Choose an existing customer and run a complimentary discovery exercise. Within days you have a ranked inventory of the AI tools actually in use.

STEP 2

Bring the report and the policy

Walk in with the findings and the AI Acceptable Use Policy template. The conversation shifts from "if" to "how," with you leading it.

STEP 3

Package the quarterly service

Wrap monitoring, quarterly reporting, policy tuning and guardrails into a recurring managed service, then repeat across your base.

Run your first discovery this quarter

See exactly which AI tools are in play across one of your customers, get the report that starts the conversation, and build the service from there. Your Barracuda partner team will help you land the first one.

