Obtainium.ai

ENGINEERED INTELLIGENCE. REAL IMPACT.

AI Agents Are Moving Fast: What the Numbers Mean for Your Business

Obtainium.ai LLC

Engineered Intelligence. Real Impact.

The Quiet Explosion Happening in AI Right Now

If you've heard the term "AI agent" lately but aren't sure what the fuss is about, you're not alone. Agents are a step beyond the AI chatbots most people already know — they don't just answer questions, they take action. They book appointments, send emails, pull data from your systems, and complete tasks end-to-end without you clicking through every step.

Here's the data that caught our attention: in January 2025, there were roughly **4,888 tools available for AI agents to use**. By February 2026 — just 14 months later — that number had grown to **177,000**. That's a 36x increase, measured empirically by the UK's AI Security Institute, not a vendor survey.

For small business owners, this isn't just a tech headline. It's a signal that the window to get ahead of competitors is open right now — and it won't stay open forever.

> *According to a study of 177,436 agent tools by the UK's AI Security Institute, the share of tools that take real-world actions grew from 27% to 65% in just 16 months. AI is shifting from information to action.*

What Is an AI Agent, in Plain Terms?

Think of a regular AI assistant like a very smart search engine — you ask it something, it tells you the answer. You still have to do the work.

An **AI agent** is different. You give it a goal, and it figures out the steps, uses the tools it needs, and completes the task. It can:

- Check your calendar and book a meeting with a new lead
- Look up a customer's history in your CRM and draft a personalized follow-up email
- Pull your last 30 days of sales data and generate a summary report
- Monitor your inbox for a specific type of message and automatically route it to the right person

The reason agents can do all of this is a technical standard called **Model Context Protocol (MCP)** — introduced by Anthropic in November 2024 and now adopted by every major AI company including OpenAI, Google, and Microsoft.

What Is MCP?

MCP is sometimes called the "USB-C for AI." Just as USB-C is a universal connector that lets you plug any device into any port, MCP is a universal connector that lets any AI model connect to any tool or data source.

Before MCP, every business system (your calendar, email, accounting software, CRM) required a custom, one-off connection to each AI tool. That was expensive and slow to build. MCP standardizes the connection once, so AI agents can now access hundreds of business systems through a single protocol.

Within six months of its November 2024 launch, MCP server downloads grew from 100,000 to over 8 million. By early 2026, that number exceeded 14 million.

What 177,000 Agent Tools Actually Reveals

The UK AI Security Institute study didn't just count tools — it categorized what they do. The findings paint a clear picture of where AI agents are actually being deployed right now.

The Shift from Reading to Doing

In November 2024, about 27% of agent tools took real-world actions — they wrote to files, sent messages, called APIs, updated records. The other 73% were passive: they read data, answered questions, retrieved information.

By February 2026, that ratio had flipped: **65% of agent tools now take actions**. Agents aren't just looking things up anymore. They're doing things.

The Most Common Tool Categories

The MCP ecosystem has developed tools across six main areas:

- **Productivity and communication** — email (Gmail, Outlook), calendar (Google Calendar, Outlook), document management (Google Drive, Notion, Box)
- **Databases and data sources** — query your business data, pull reports, cross-reference records
- **Development and automation** — connect to business APIs, trigger workflows, automate repetitive processes
- **Customer engagement** — CRM integration (Salesforce, HubSpot), scheduling, support

ticket routing

- **Financial operations** — invoice tracking, payment status, expense categorization
- **Search and research** — web search, competitor monitoring, news tracking

Payments Are Moving Into Agents Fast

One data point worth noting: MCP servers with payment execution capabilities grew from **47 servers in January 2025 to 1,578 by February 2026** — a 33x increase in one year. The Bank of England collaborated on this part of the study, signaling that governments and financial regulators are already paying attention.

For small businesses, this trajectory matters: the systems that handle your invoices, subscriptions, and payments are becoming agent-accessible. That creates both opportunity (automated collections, smarter billing) and responsibility (making sure the right controls are in place).

What This Means for a Small Business Owner Today

You don't need to understand protocols or AI infrastructure to benefit from agents. What you need to know is what they can actually do for you — and what's realistic to expect in 2026.

Tasks Agents Are Already Handling for Small Businesses

Customer inquiries and scheduling

AI agents now handle 60–80% of routine customer inquiries without human intervention. For a service business fielding calls about hours, availability, and pricing, an agent can answer, check the calendar, and book the appointment — without you or your staff touching it.

Lead follow-up

An agent can monitor your email inbox for new lead notifications, look up the lead's business in your CRM, draft a personalized follow-up email based on their industry and inquiry, and flag it for your review before sending. One workflow, zero manual steps.

Invoicing and bookkeeping assistance

Agents connected to accounting platforms can monitor outstanding invoices, send payment reminders (calibrated by customer relationship — firmer tone for new clients, softer for long-term ones), and generate weekly financial summaries. Businesses using AI-assisted bookkeeping report 70–80% reductions in time spent on financial admin.

Appointment confirmations and reminders

For service businesses, the gap between booking and showing up costs money. Agents can send automated confirmations, reminders 24 hours before, and re-engagement messages for no-shows — all connected to your actual calendar data.

Research and competitive monitoring

Agents can scan news, industry publications, and competitor websites on a schedule and deliver a summary to your inbox every Monday morning. What used to take an hour of browsing now takes zero time.

What Agents Cannot Do (Yet)

Being clear about limitations matters as much as the possibilities:

- Agents are not infallible. They make mistakes, especially with ambiguous instructions or unusual edge cases.
- Complex judgment calls — a difficult client negotiation, a strategic pricing decision — still need a human.
- Security must be deliberate. Agents with access to your systems are only as safe as your setup. Credentials, permissions, and audit trails need proper configuration.
- The technology is evolving fast. What's difficult today may be straightforward by the end of 2026.

How to Think About Getting Started

The 36x growth in agent tools isn't a reason to panic — it's a reason to get informed now, before your competitors do. Here's a practical framework for approaching agents as a small business owner.

Step 1: Identify Your Highest-Repetition Tasks

Agents deliver the most value where work is predictable and rule-based. Make a list of tasks your team does every week that follow the same pattern — answering the same questions, sending the same types of emails, pulling the same reports. These are your best candidates.

Common starting points:

- New lead intake and routing
-

Appointment scheduling and reminders
- Invoice follow-ups
- Weekly reporting
- Customer FAQ responses

Step 2: Start with One Connected System

The biggest mistake businesses make is trying to automate everything at once. Pick one system you already use — your calendar, your inbox, or your accounting software — and explore what an AI agent can do with just that one connection.

Getting one workflow working well teaches you more than reading ten articles. It also builds the trust and comfort you'll need to expand.

Step 3: Audit What Permissions You're Granting

Before connecting any AI agent to a business system, ask three questions:

1. What data can this agent read?
2. What actions can this agent take?
3. Who can see what the agent did?

This isn't about fear — it's about good business practice. The same due diligence you apply to any software tool applies here.

Step 4: Measure the Time Saved

Before you deploy an agent, track how long the manual process currently takes. After two weeks with the agent running, compare. Concrete time savings are the best argument for expanding — and the clearest indicator when something needs adjustment.

The Bigger Picture

The 36x growth in agent tools is not a bubble or a trend — it's infrastructure being built. Every major technology company has adopted the MCP standard. GitHub's top 10 most-watched new repositories in the first half of 2025 were all focused on agent tooling and MCP integration.

In 2023 and 2024, AI was about generating text. In 2025 and 2026, AI is about taking action.

The businesses that understand this distinction — and start building workflows that leverage it — will have a meaningful operational advantage over those that don't.

You don't have to be a technology company to benefit. You just have to be willing to ask: "Where does my team spend time on repetitive work that an agent could handle?"

That's where the opportunity lives.

Key Takeaways

- **AI agents act, not just answer.** The shift from information retrieval to real-world action happened faster than anyone predicted — 65% of tools now take actions, up from 27% in late 2024.
- **The ecosystem is massive and growing.** 177,000 tools in 14 months means businesses have more ways to connect agents to their existing systems than ever before.
- **The best starting point is your most repetitive task.** Scheduling, lead follow-up, invoice reminders, and weekly reports are proven entry points for small businesses.
- **Security and oversight matter from day one.** Know what your agent can access and document what it does.
- **You don't need to move fast — you need to move smart.** Pick one use case, prove the value, then expand.

Next Steps

If you're curious about which AI agent use cases make the most sense for your specific business, we offer a free AI Readiness Audit. We'll assess your current operations, identify the highest-value automation opportunities, and give you a plain-language roadmap — no jargon, no pressure.

Visit obtainium.ai to learn more or book a consultation.