FOR THE PERSON WHO HAS TO APPROVE THIS

Your AI assistants can reach everything your staff can reach

Including the files that were shared too widely years ago. That exposure is not new. What is new is that it now answers questions.

WHAT IS HAPPENING

People across the business are building AI agents, in Microsoft 365, without going through IT. Each one runs at the access of whoever built it.

That access was granted for a person doing a job, not for a standing capability that answers anyone who asks it. Nobody approved it for this purpose, because nobody was asked.

When the person who built an agent changes team or leaves, the agent keeps running. Gartner expects the average Fortune 500 enterprise to be running more than 150,000 agents by 2028, up from fewer than 15 in 2025.

WHAT IT COSTS

Audit exposure first. Regulators now ask what AI systems the organization runs, what they reach, and who approved them. Those questions are answerable or they are not.

Then remediation. Fixing access across thousands of workspaces after an incident costs multiples of what it costs to see it beforehand, and it lands on the team least able to absorb it.

Then the delay to the AI program itself. When nobody can say what an agent reaches, the safe answer to every rollout request is no, and the investment stalls while the risk stays.

WHAT GOOD LOOKS LIKE

A complete inventory. Every agent and connected app, with a named owner and a plain statement of what data it can reach.

Approval before exposure. One check between an agent being built and an agent being shared, light enough that people still build.

Continuous review rather than an annual cleanup, with the evidence produced on demand instead of assembled for each audit.

USD 6m

Average cost of a breach where AI was involved in the attack, against USD 4.99 million overall.

IBM Cost of a Data Breach Report 2026

Specialist Risk Group grew from 119 staff to 450 through acquisition, each one bringing its own accounts and data into the same Microsoft 365 estate. Their infrastructure lead described the problem before they fixed it: "there is no way to view it in one place in a simple contextual way."

Greg Bowles, Infrastructure Team Leader, Specialist Risk Group

What we are asking for

Thirty minutes to walk through what is actually running in our tenant, and what each one can reach. Not a purchase decision and not a procurement conversation.

If the answer turns out to be that we already know, that is a thirty-minute meeting well spent. If it turns out that we do not, it is better to find that out now than during an audit or after an incident.

Rencore inventories the digital workplace, the apps and automations teams build, and the AI agents that reach company content. You see what each one can reach, then set the rules it follows, across Microsoft 365, Power Platform, and Microsoft's AI stack. Independent and third party, a Microsoft Partner, and software built in the EU. Rencore governs more than 2.5 million users across the Microsoft estate.