What is Shadow AI, and who inside my organization is creating the risk?

Short answer: Shadow AI is employees using AI tools that IT hasn't approved or doesn't know about. The risk isn't limited to rank-and-file staff — privileged administrators and compromised accounts are often the larger exposure.

Three sources of exposure

- **Employees** using unsanctioned AI tools for everyday productivity.
- **Privileged administrators** whose high-level access means anything they feed an AI tool can include highly sensitive corporate data.
- **Compromised accounts**, where an attacker with valid credentials uses AI tools as an exfiltration channel — traffic that looks like ordinary productivity.

This is already happening

Cyber Crucible has directly observed mass access to large volumes of data at once by employees using AI tools to search for and upload information. This isn't a theoretical future risk being modeled; it's behavior visible in real deployments today.

The third category deserves particular attention. An attacker using AI tools to move data out is difficult to distinguish from an enthusiastic employee — unless enforcement happens at the data-access layer, where intent and policy can be evaluated regardless of who is logged in.

Revision #3
Created 2026-07-20 19:23:57 UTC by Dennis Underwood
Updated 2026-07-21 19:32:13 UTC by Dennis Underwood