

AI Control Center

Risks Posed by AI Agents

For many companies, agentic AI has expanded from a pilot program managed by IT to an integral productivity enhancer. Among small- and medium-sized businesses, [62%](#) of SMB leaders are very confident about giving high-stakes tasks to AI agents, and one in three consider agentic AI mission-critical.

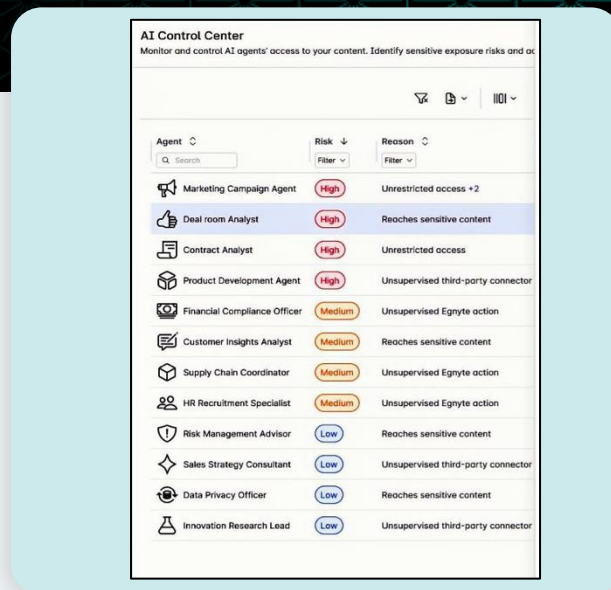
Agentic AI adoption is increasing across project-driven industries and organizations that manage sensitive data, from financial services firms to construction companies. Unfortunately, every connected agent creates a new way for sensitive content to be exposed.

In addition, governance of agents has not kept pace with their adoption. According to published reports, only [13%](#) of companies believe they have the proper agentic AI protection in place, and [more than half](#) of organizations have experienced agentic AI scoping violations.

Businesses need to address real-world gaps, such as:

- IT admins can't determine which agents are connected to their content, and checking each agent's configuration individually doesn't scale.
- Even when an agent's connectivity is visible, it's difficult to determine whether the agent can reach sensitive data such as Personally Identifiable Information (PII).
- Without such clarity, teams cannot tell whether PII, healthcare, or financial data is exposed. This results in compliance and data security risk.
- Agents often inherit users' broad data access and permissioning, enabling agents to reach content far outside of their intended scope.

Egnyte AI Control Center provides Data Security, Compliance, and IT teams with the confidence they need to deploy new agents safely, reduce risk, and keep pace with AI adoption. Stakeholders also get immediate visibility into potential risk and can adjust an agent's data access, in just a few clicks. [Request a demo](#) now to learn more.



Manage Risk With AI Control Center

Egnyte AI Control Center gives IT admins a single place to see, map, and control AI agents' access to sensitive content. Admins can discover every connected agent, understand the sensitive data that the agent can reach, and activate new agents safely and securely, without deploying technology outside of Egnyte's content platform. Because AI Control Center builds upon Egnyte's proven sensitive content protection capabilities, admins can focus on remediating the riskiest agents that have gained access to your most sensitive data.

Key AI Control Center Capabilities:

- Identify every connected AI agent that has access to sensitive data, including PII, corporate IP, healthcare data, and financial services information.
- Adjust agents' access to the correct Egnyte folders, so agents only see the content that they need to see.
- Create AI Safeguards policies for ongoing sensitive content protection.