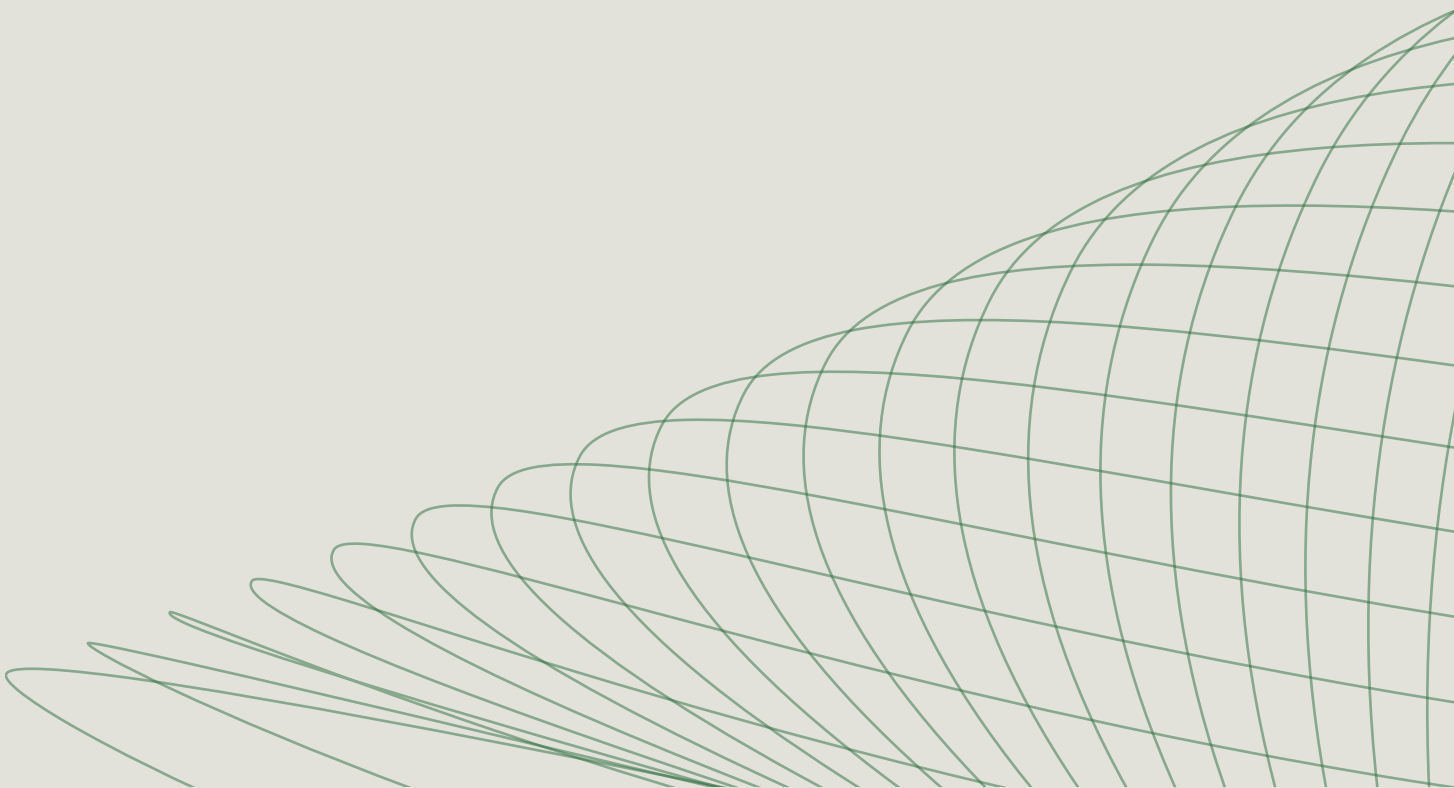
STACKLOK

RESEARCH REPORT

State of Model Context Protocol in Retail 2026



Contents

Introduction

In December 2025, we surveyed 300 senior technical leaders across large enterprises in three specific industries: **RETAIL, FINANCIAL SERVICES** and **SOFTWARE**. This report focuses on **RETAIL**, with respondent titles largely being CTO, Principal Engineer or Director of AI Platform. As a requirement, all respondents had significant decision-making ownership of AI investments.

In our survey, we specifically asked respondents about their organization's adoption of the Model Context Protocol (MCP). We wanted to understand their progress, use cases, obstacles and more. Following is a summary of the results for those **RETAIL** leaders, so that you can see how you compare to industry peers (as well as peers in **FINANCIAL SERVICES** and **SOFTWARE**). Note that we're intentionally avoiding subjective commentary and sales pitches; we figure you're here because you want the benchmarking data points.

Model Context Protocol

On the chance that MCP is new to you, here's a brief primer. In November 2024, Anthropic introduced MCP as a 'USB-C' to connect AI agents, assistants and models to the resources and tools needed to take real action. MCP allows probabilistic AI agents to talk to deterministic systems.

When connected to the right MCP server(s), AI agents can do things like, submit a GitHub pull request, pull and present data from an Oracle database, update the company website and much, much more. MCP is being viewed and used as a means for enterprises to multiply the value of their AI agents, assistants and models.

Of course, given the connection to sensitive systems, MCP requires real scrutiny. It's imperative that enterprises (and individuals) using MCP have the right security and policies in place to use MCP safely. The ability to secure MCP to enterprise standards is still maturing, and that was a driving factor in designing this study; we wanted to understand whether enterprises were getting stuck, or whether they were overcoming obstacles to use MCP in production.

Respondent Profile

Geographies

This was not a global study; as a first research effort it was simply beyond our scope. 78% of respondents were based in the United States, 12% were based in Canada, and the remaining 10% were based in the UK.

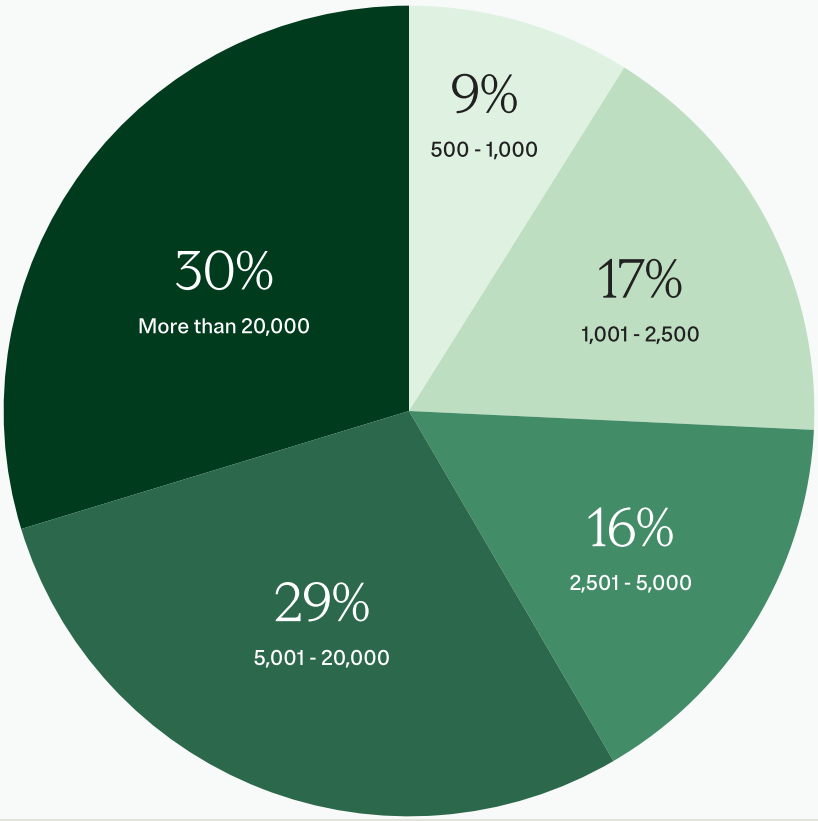
Industries

We collected 100 responses from senior technical leaders in each of three industries: Financial Services, Retail and Software. We viewed these as three very different industries, and we wanted to understand how their varying priorities and historical approaches to technology adoption would affect their embrace of MCP.

Organization Size

The study targeted large enterprises; nearly 60% of respondents worked for companies with more than 5,000 employees.

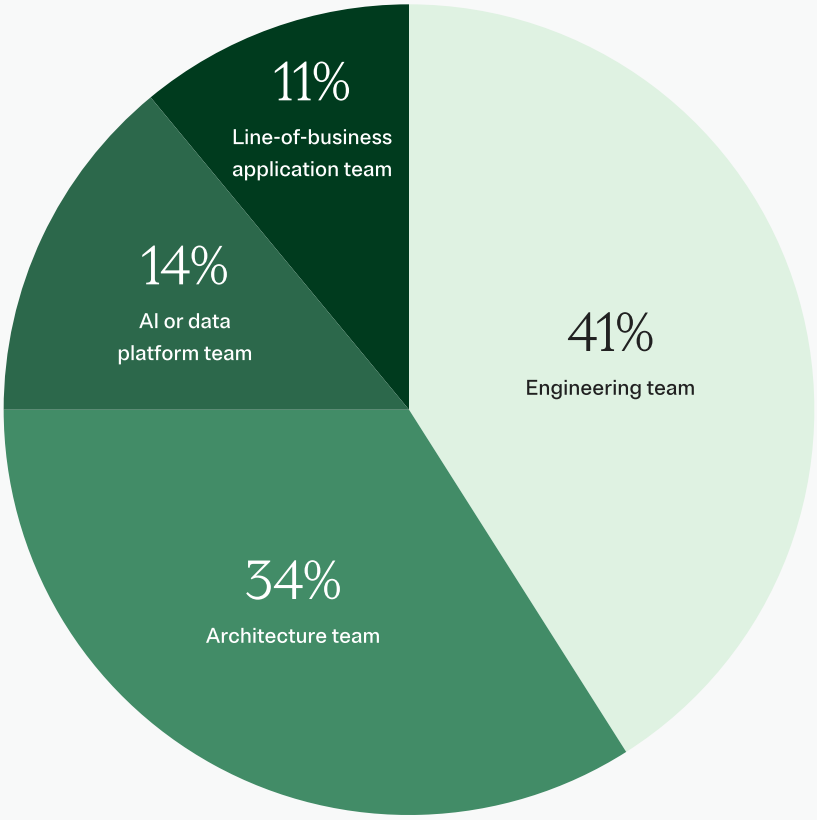
"Approximately how many employees work at your organization?"



Respondent Role

Study respondents were deeply involved in AI technology decision-making. More than half of respondents noted ownership of all of the following: investigating options, technical evaluations, technology selection and implementation. All respondents had senior titles (Director-and-above or equivalent) and reported up as follows:

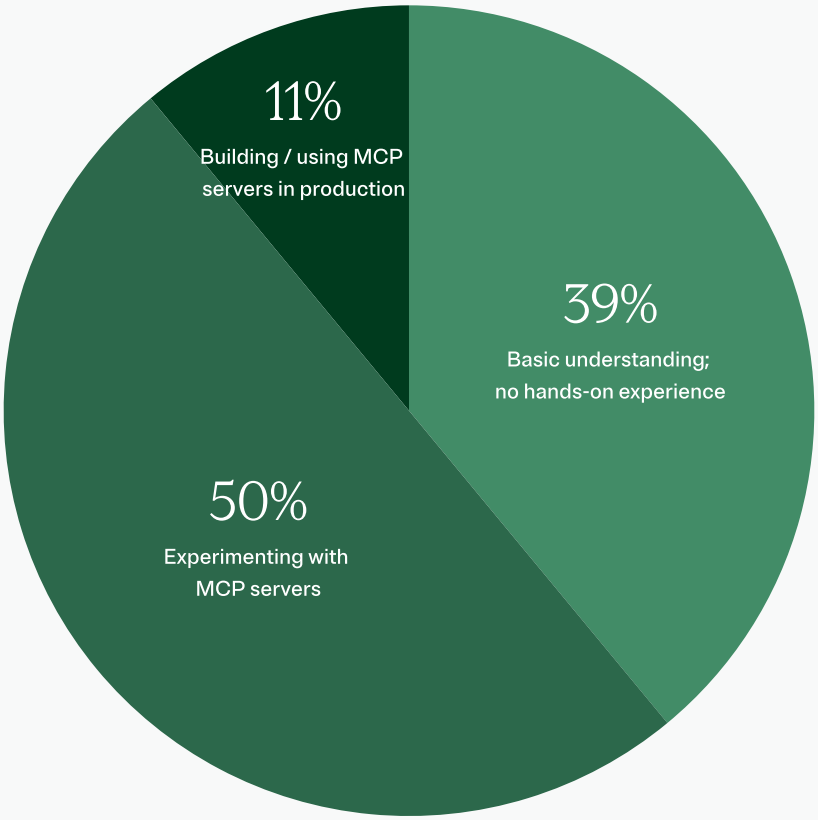
"How would you characterize your team?"



MCP Experience

Finally, we asked respondents about their familiarity with MCP:

"What is your level of familiarity with MCP servers?"



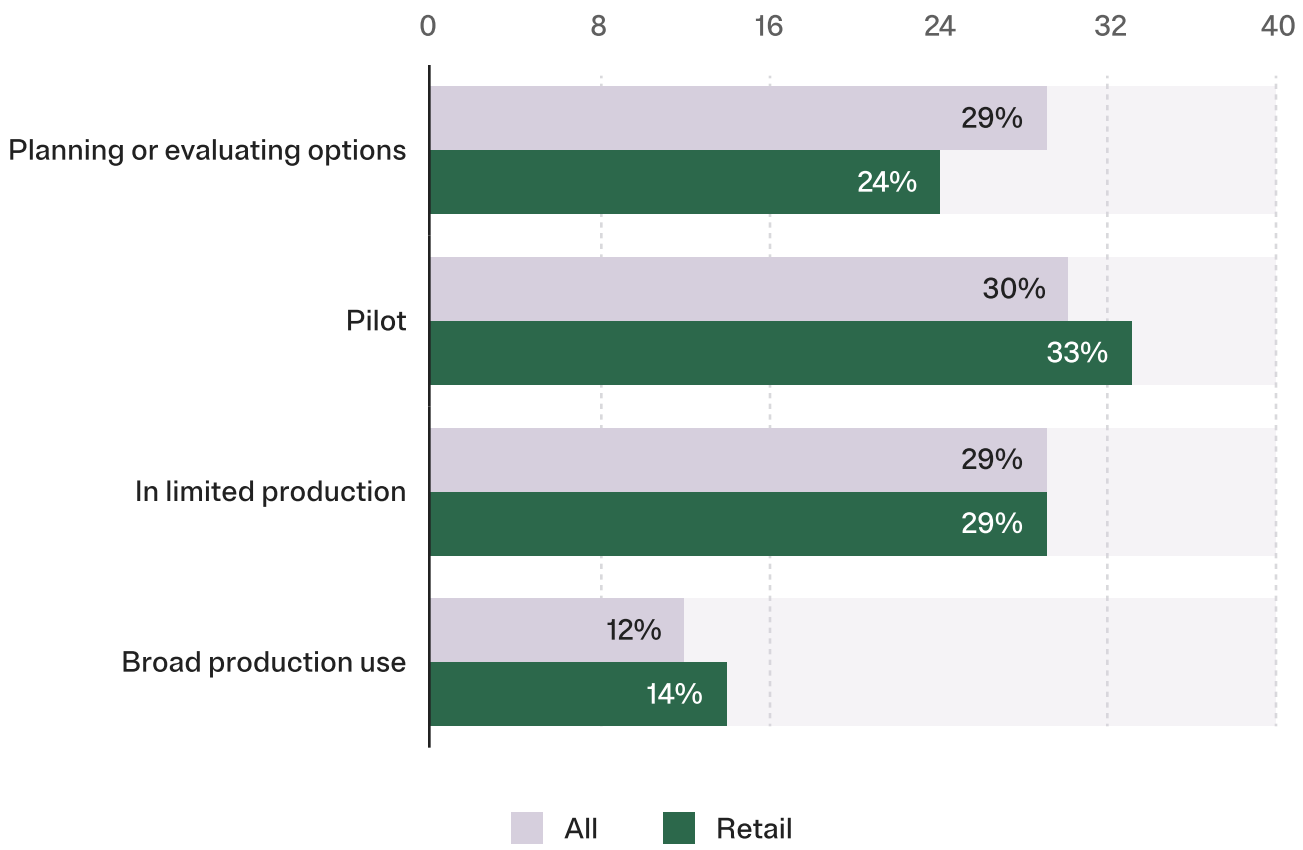
Anyone who did not meet our requirements for organization size, role seniority, etc. was filtered out. And with that, we dove into the study.

MCP Progress

Usage and Use Cases

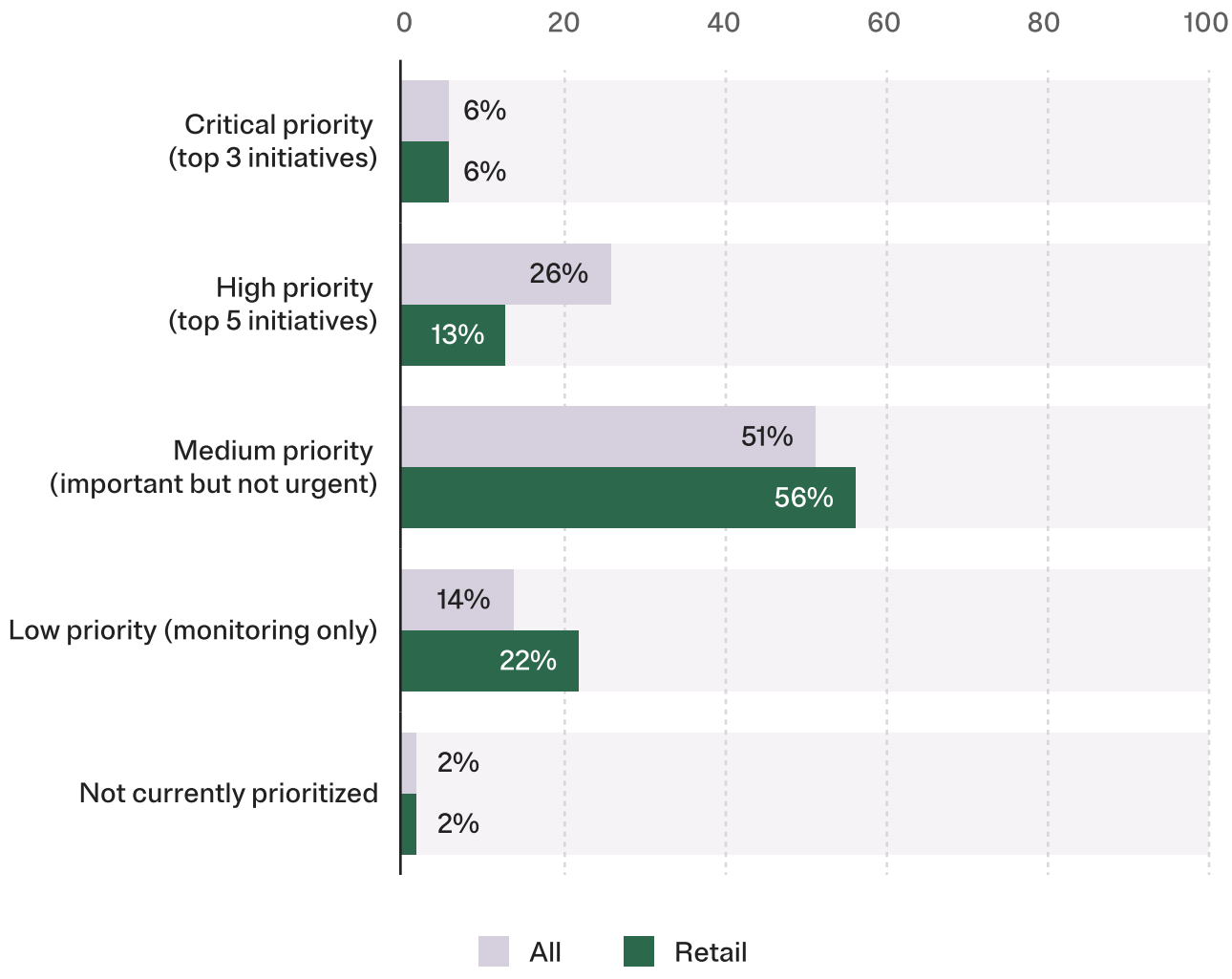
First things first, we needed to establish where respondents were in their MCP adoption journey. **RETAIL** respondents mirrored cross-industry averages, though they were more likely to be in broad production than peers in **FINANCIAL SERVICES.**

"Which of the following best describes your organization's current adoption of MCP servers?"



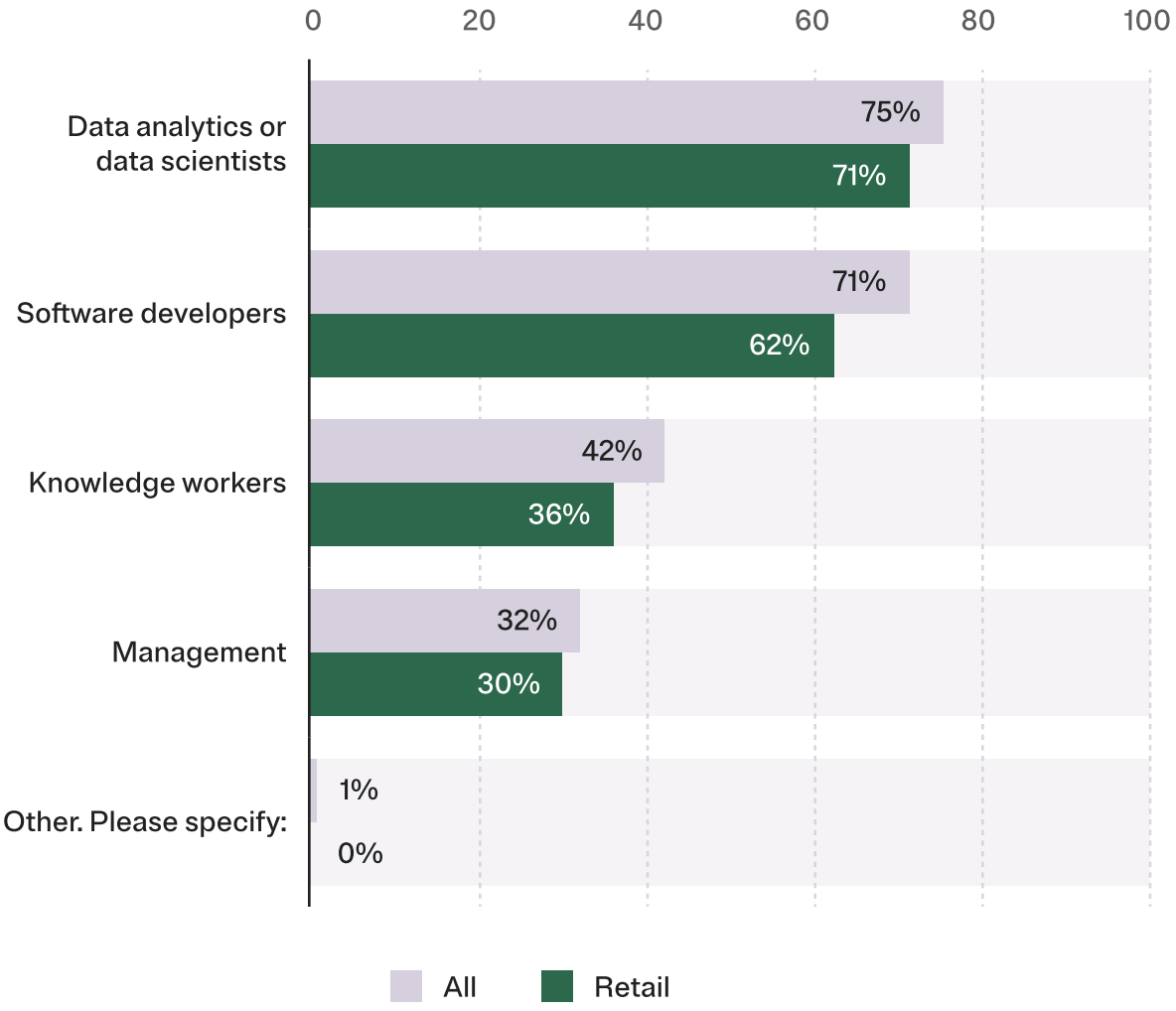
We wanted to know where MCP adoption ranked in relative priority to other technology investments. Approximately one-in-five **RETAIL** respondents acknowledged MCP adoption as a top-5 priority (Critical + High), which was less than other industries. Regardless, just one year after its introduction, it's remarkable that MCP is a top 5 priority at so many enterprises; this speaks to the power of MCP to unlock value in other AI investments.

"How has your organization prioritized MCP adoption relative to other technology investments?"



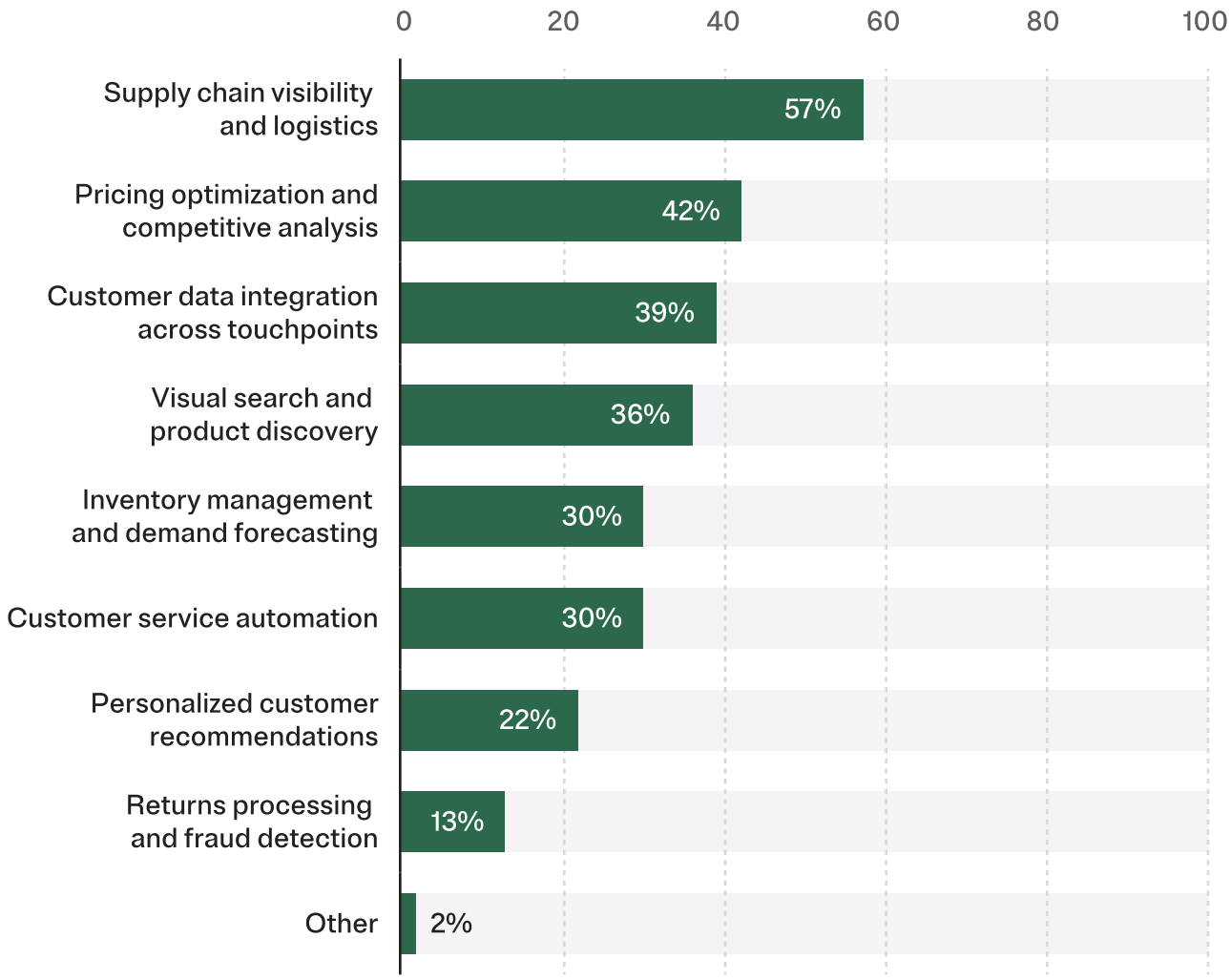
And then we started to dig into users and use cases. In **RETAIL**, intended users were most likely to be data analysts and data scientists.

"Who are (or are expected to be) the primary users of MCP servers at your organization?"



RETAIL firms shared a broad set of intended use cases for MCP, with emphasis on making more data better available to inform supply chain and pricing decisions. There's also recognition that MCP could tie customer data together across touchpoints to enable AI agents to personalize customer experiences and more readily resolve customer issues.

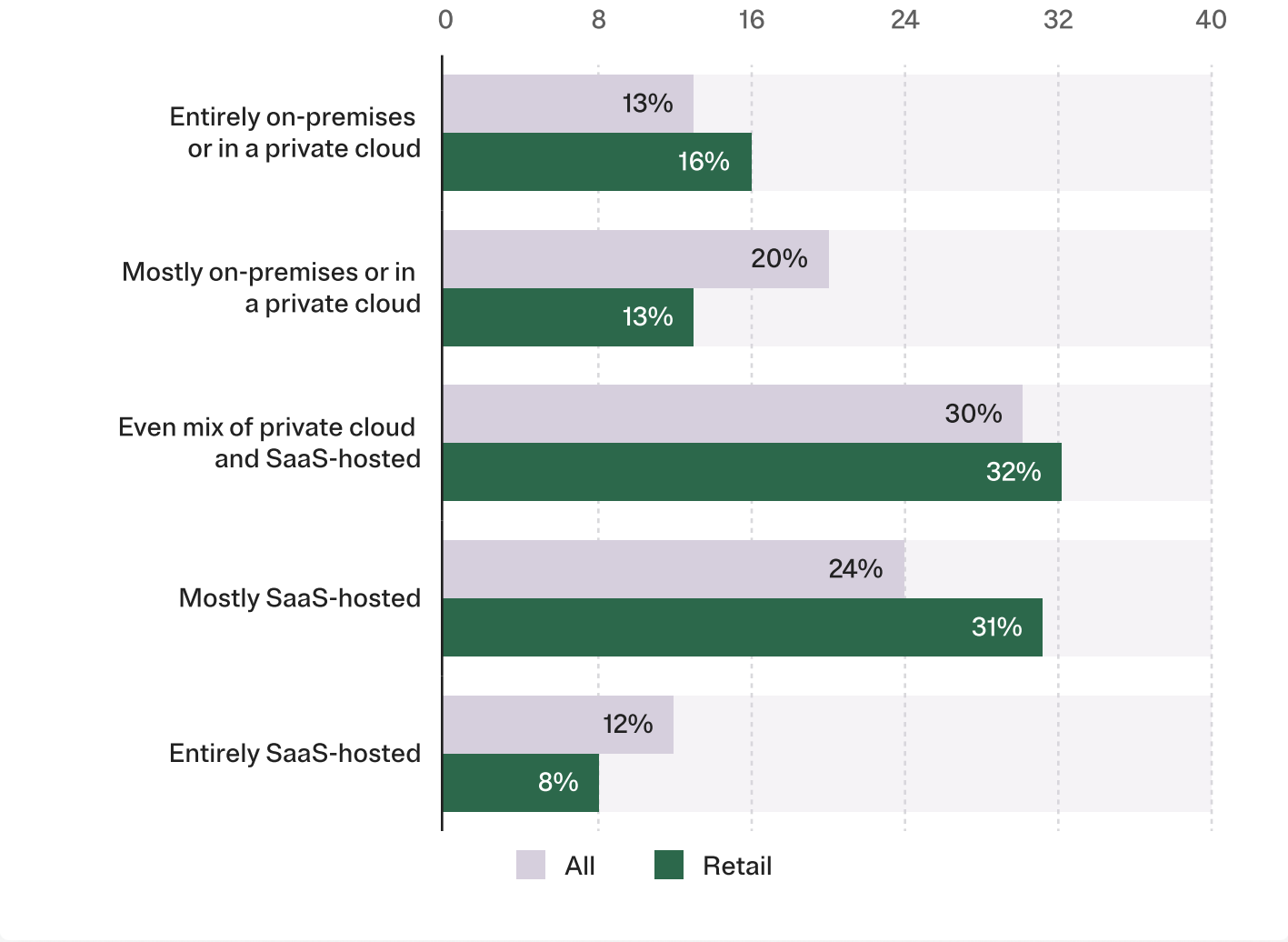
"What are the use cases for MCP in your organization? Choose all that apply."



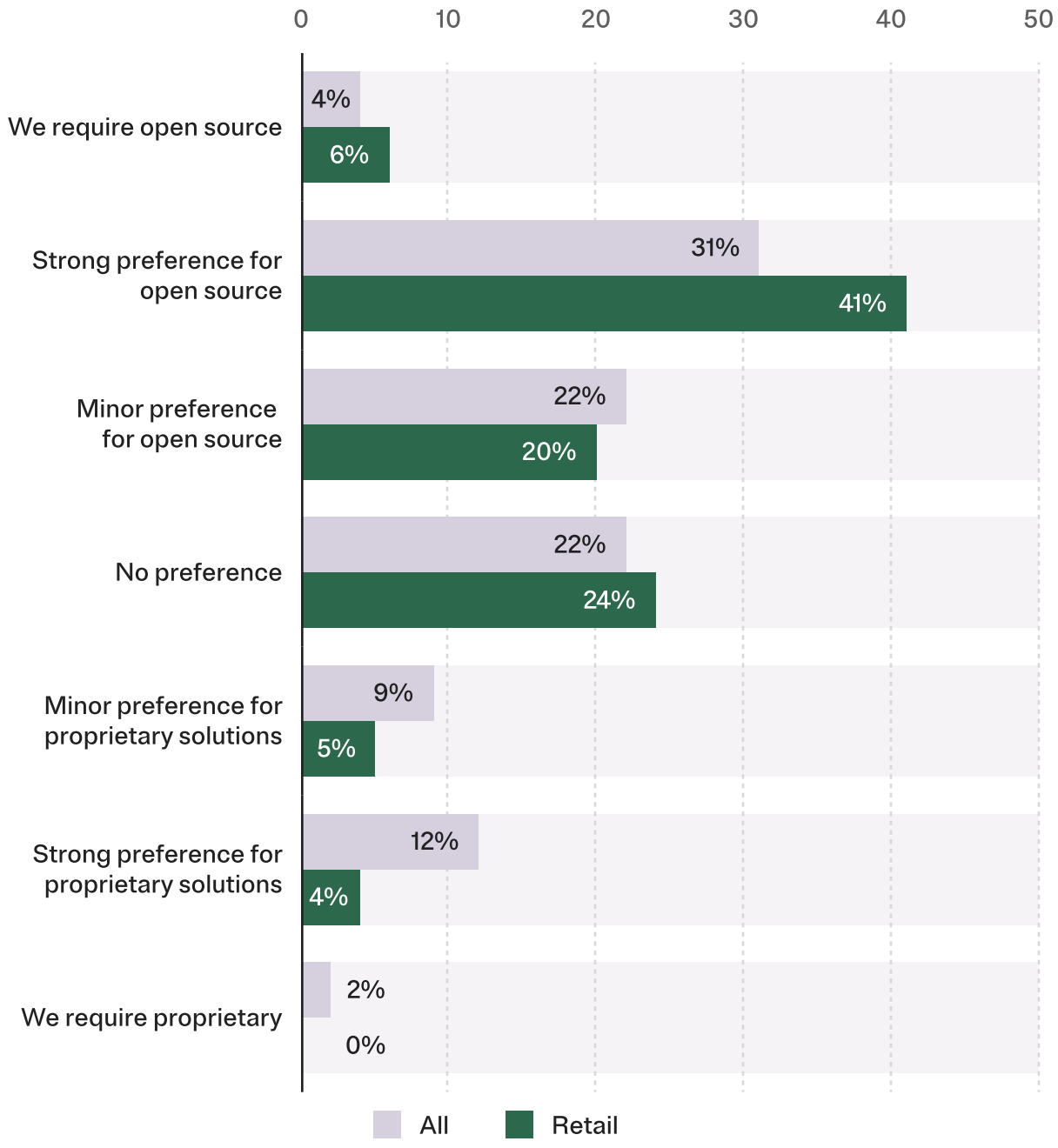
Technical Considerations

Enterprises adopting MCP have to figure out how it fits into their environment; so, we asked a series of questions about technical considerations. **RETAIL** organizations were more likely to (a) prefer open source over proprietary solutions, and (b) build their MCP platform in-house using open source technologies.

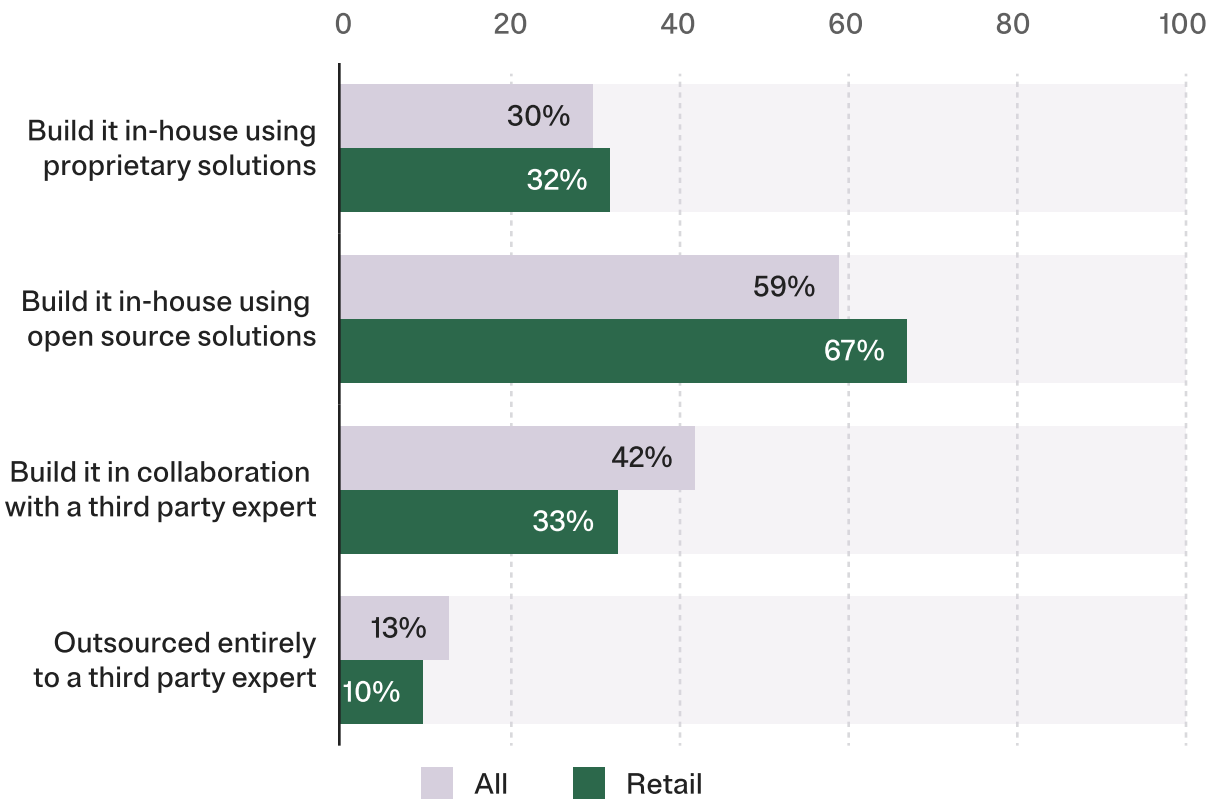
"Where are (will) your MCP servers (be) hosted?"



"Does your team have a preference for the type of MCP platform you adopt?"



"How has your organization built or planned to build your MCP platform?"

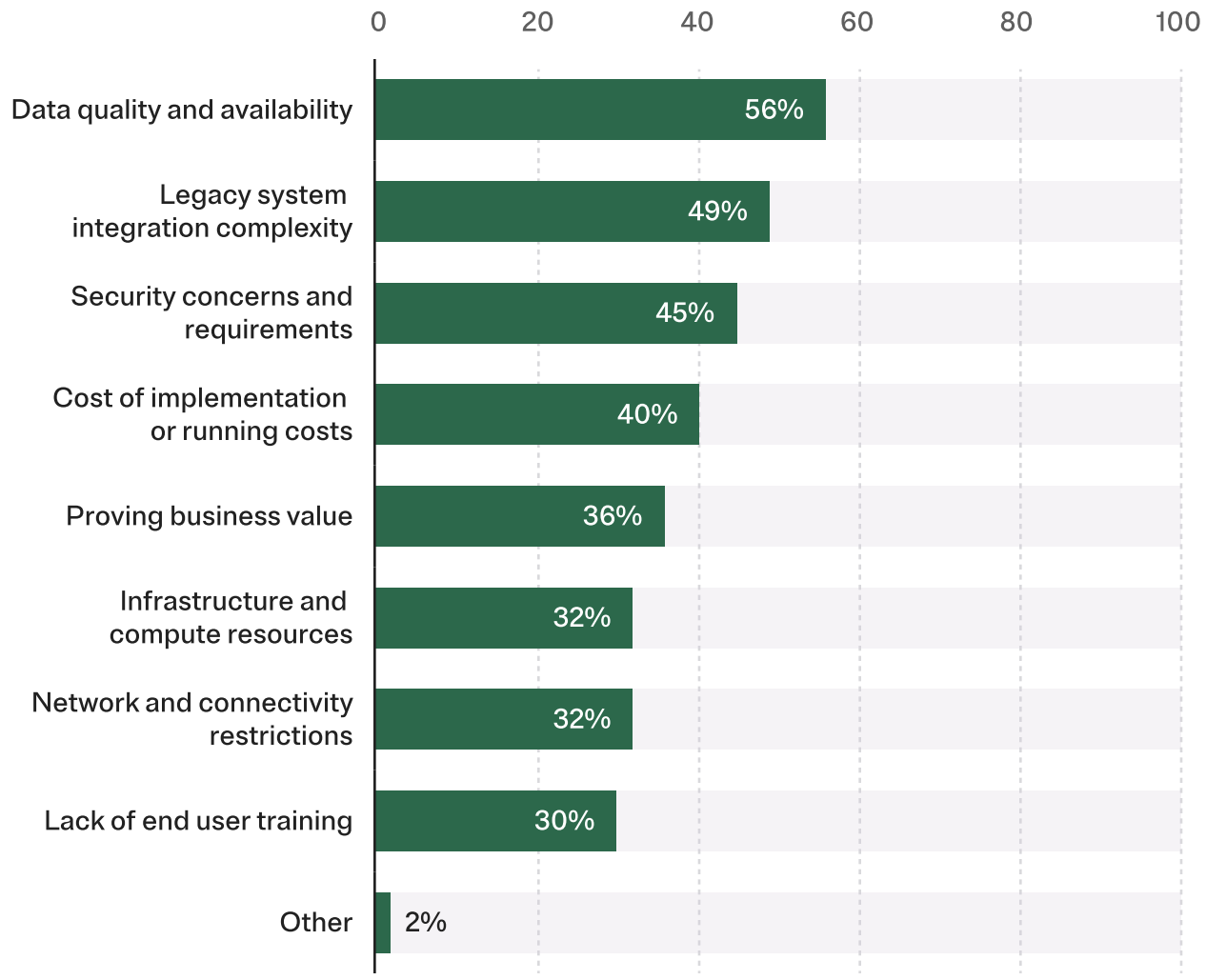


All this talk of technology and the challenges with deploying any solution in a fast-moving market provides a nifty segue to talk about MCP pain.

MCP Pain

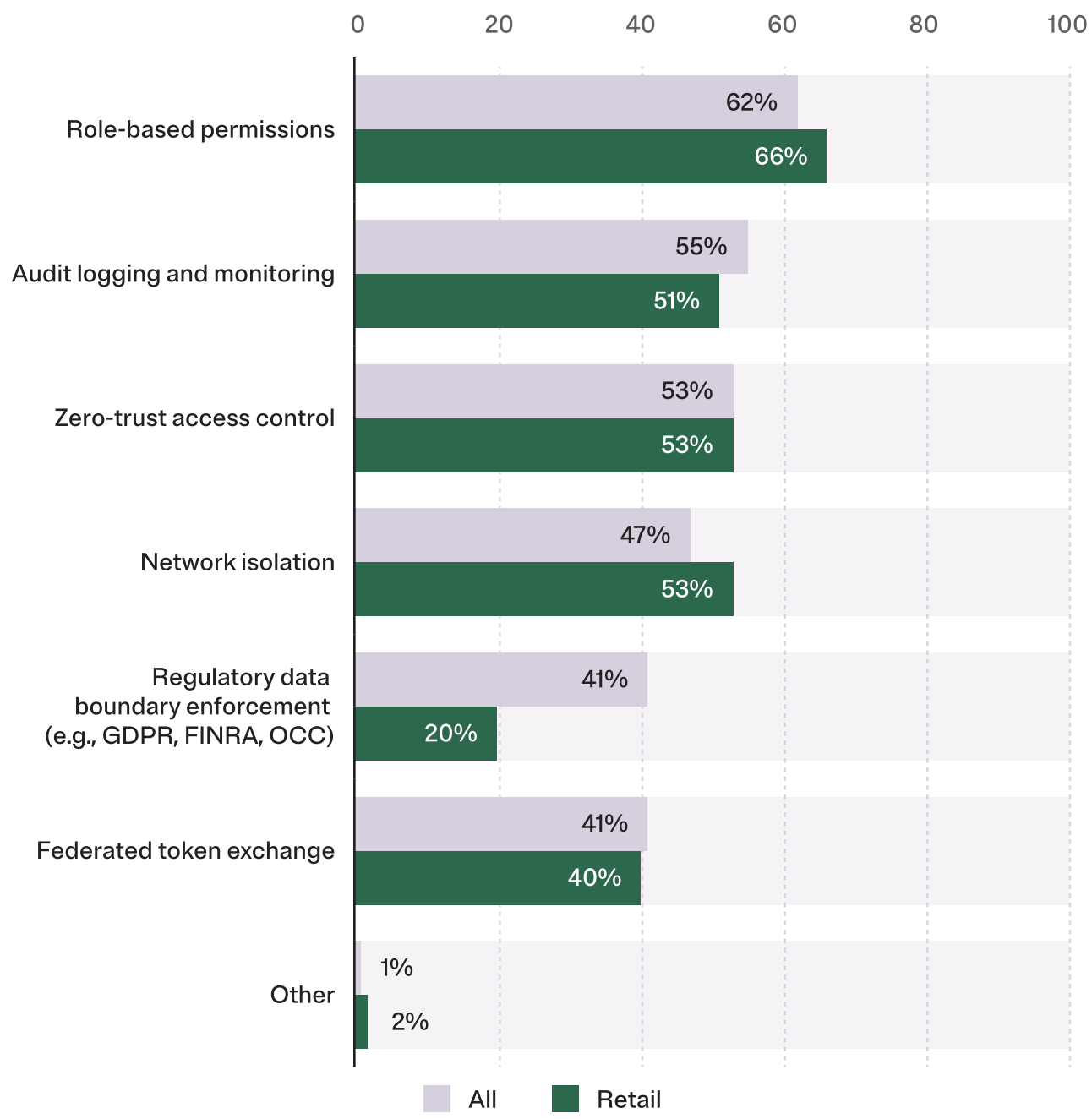
We asked **RETAIL** respondents, "What obstacles are blocking or slowing MCP adoption in your organization?" and allowed them to choose all applicable options. Whereas respondents in **FINANCIAL SERVICES** and **SOFTWARE** selected security concerns as the top issue, RETAIL respondents continued to emphasize data issues. Challenges with data quality and availability are obstacles that have to be addressed to unlock data-centric use cases.

"What obstacles are blocking or slowing MCP adoption in your organization?"



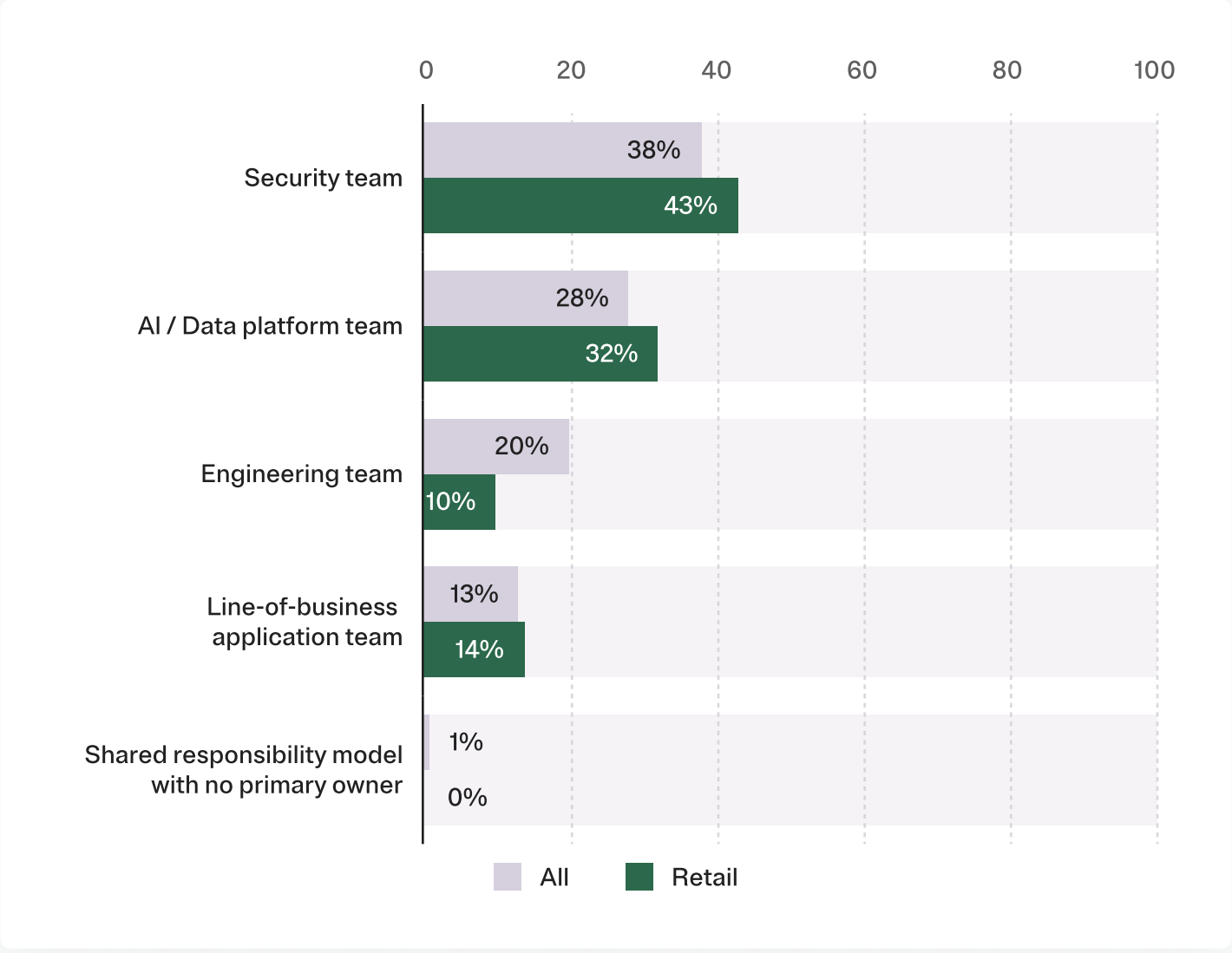
Given that security was near the top of the list of obstacles, we asked respondents about the measures they were putting in place to use MCP safely. **RETAIL** firms are leaning on a variety of security layers, with slightly higher use of RBAC and network isolation than in other industries.

"Which of the following security measures are applied to your organization's use of MCP servers?"



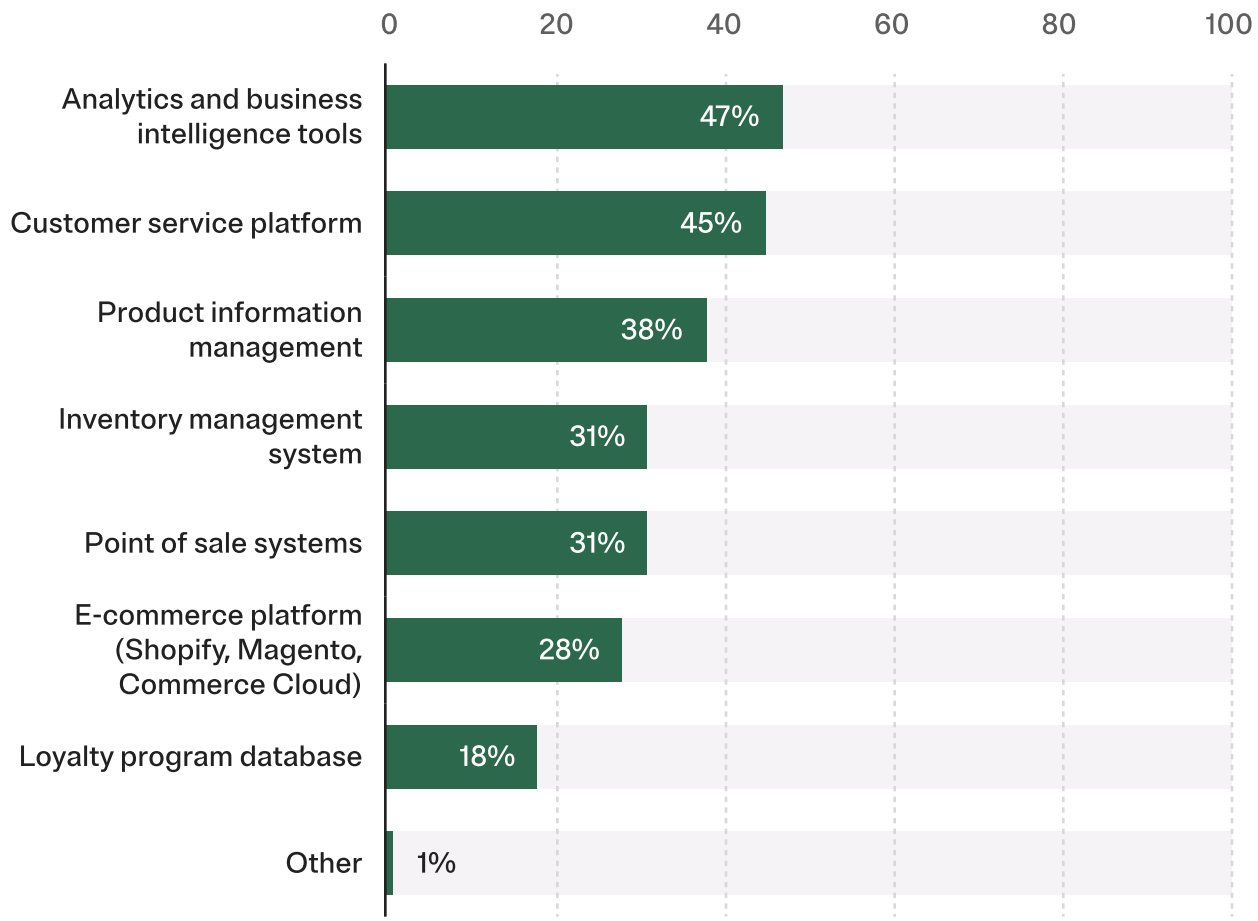
An important follow-up question in the study asked participants who was accountable for managing MCP security and compliance. The Security team was acknowledged as the primary owner, and in **RETAIL** it was less likely that Engineering had a role to play with security than in other industries.

"Who primarily manages security and compliance for your MCP deployment?"



Near the top of the obstacles list was "legacy system integration" and "cost of implementation". Figuring out where the hang-ups are / will be is valuable to those on an MCP adoption journey. **RETAIL** firms are working hard to connect a broad swath of systems to AI agents via MCP, but consistently featuring data analytics and customer service tools.

"Which systems are you trying to connect to AI agents using MCP? Choose all that apply."



Conclusions

RETAIL leaders see Model Context Protocol as a high-impact enabler for AI, particularly as a way to turn data into knowledge that can be applied to supply chain and pricing decisions. MCP also offers the potential to integrate more customer data so retailers can offer personalized experiences at scale.

While MCP is already a top-five priority for many enterprises, production use lags due to data quality and availability, in addition to security obstacles. Success in **RETAIL** hinges on secure, governed, enterprise-grade MCP deployments that can safely connect AI to critical internal systems.

About Stacklok

Stacklok offers the most complete and secure MCP platform for enterprises to use in production. Customers take complete control of their MCP estate, so employees and their AI agents can access the context and tools they need, and admins have full oversight and centralized management. Stacklok also maintains the popular open source MCP platform, ToolHive along with Red Hat and a growing community of contributors. The company is founded and led by Craig McLuckie, a co-creator of Kubernetes and the Cloud Native Computing Foundation.

Learn more about Stacklok:

www.stacklok.com

Explore our GitHub repo:

https://github.com/stacklok

Engage with us via Discord

https://discord.gg/stacklok

Get in direct contact with an Applied MCP Engineer

enterprise@stacklok.com