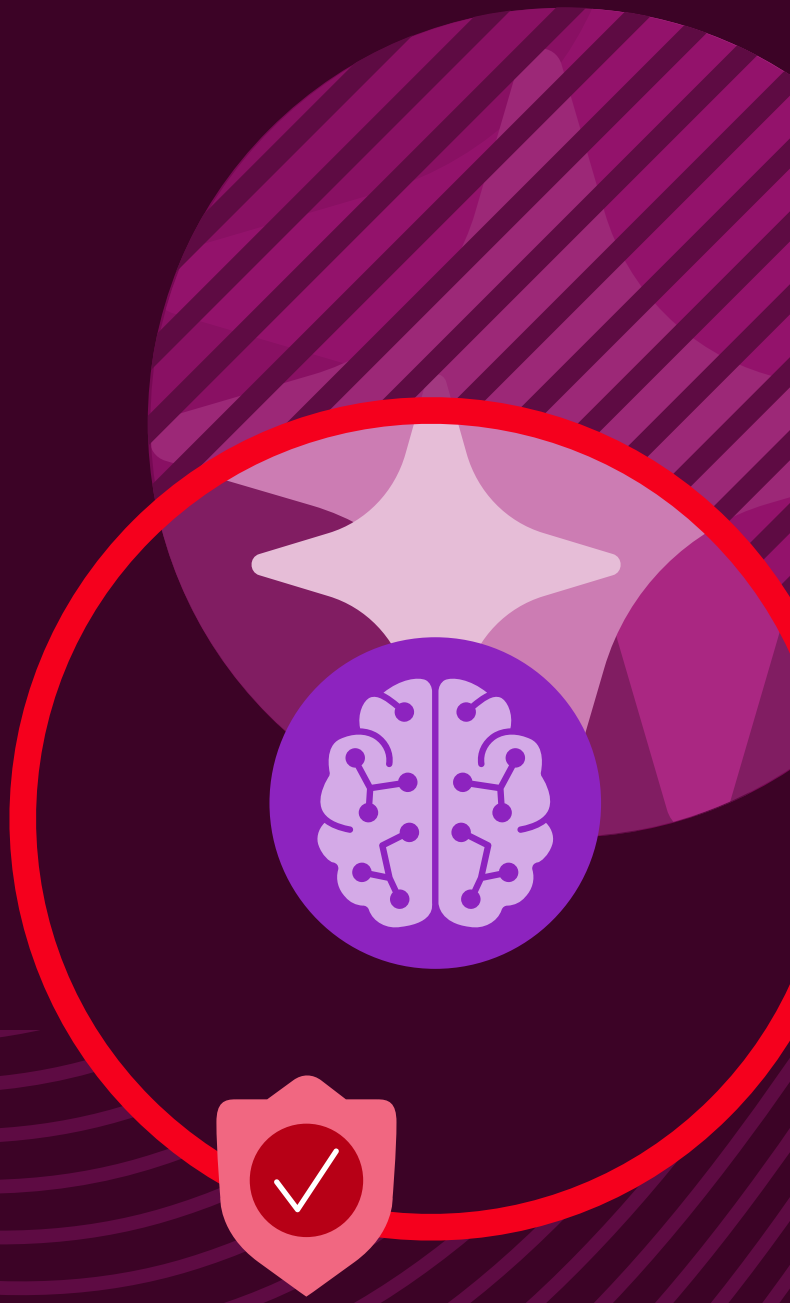
State of AI Application Strategy Report 2025

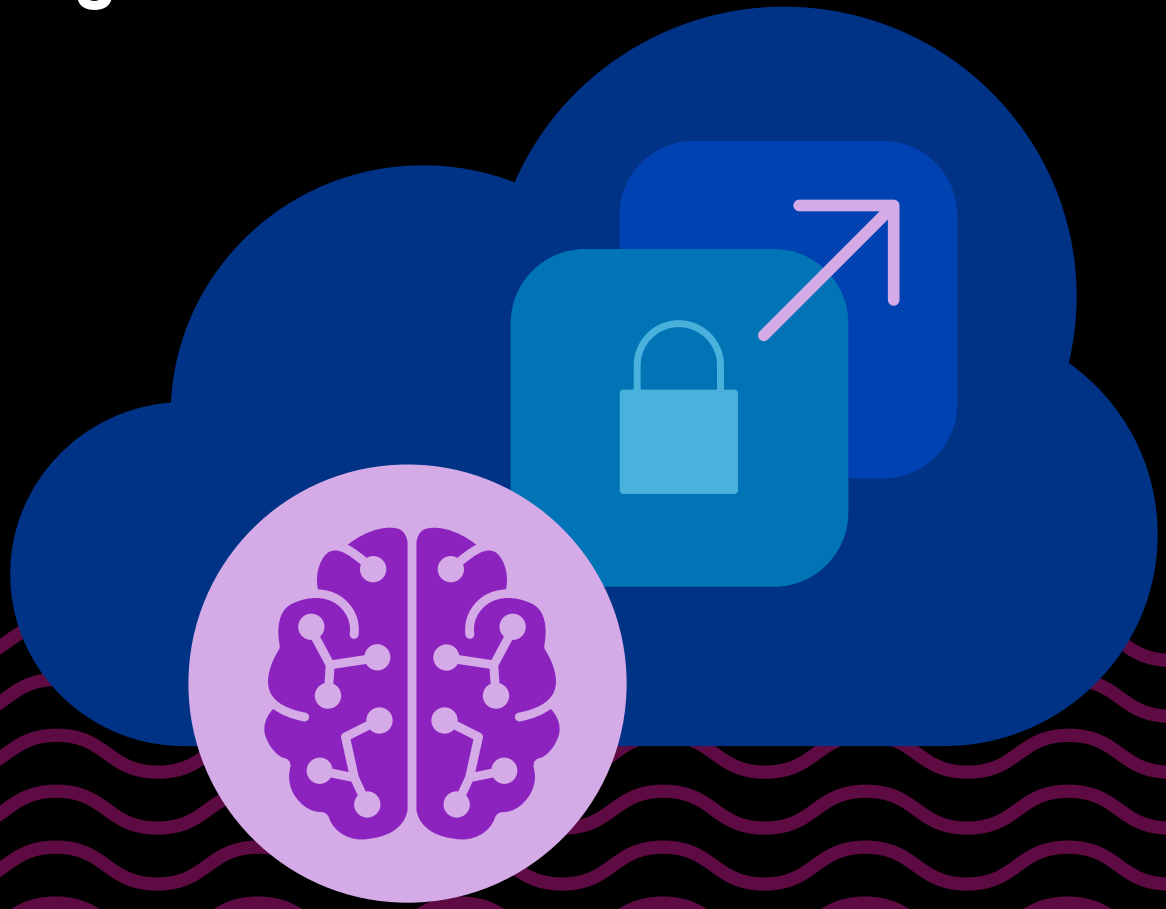
AI Readiness Index: Assessing Operational Preparedness for Enterprise AI



Contents

Introduction:

Index Methodology and Key Findings

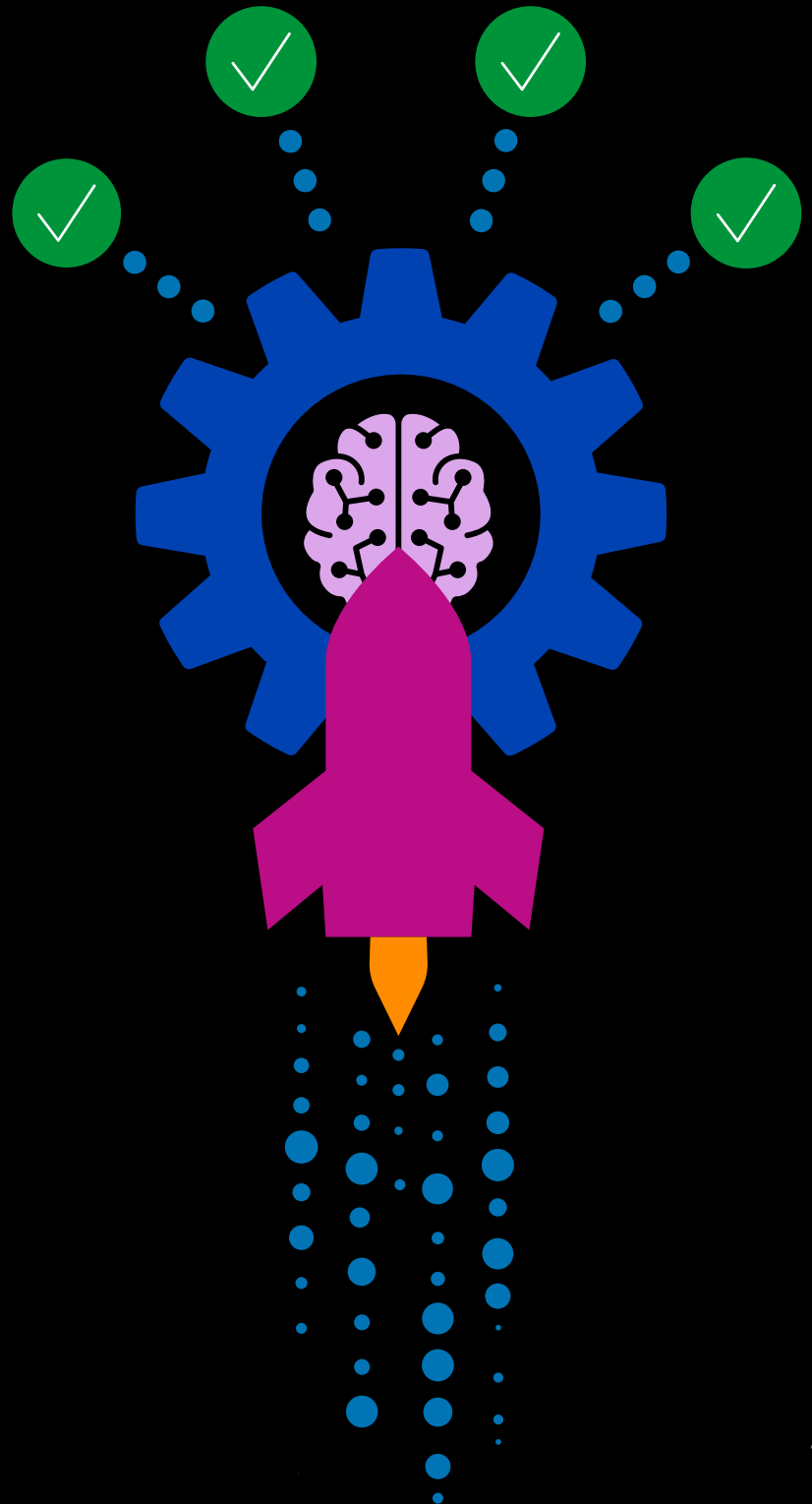


The AI era is now. As revealed by the F5 2025 State of Application Strategy Report, 96% of organizations are deploying AI models, and virtually no organization today can move into the future without considering how machine learning (ML) and intelligent apps might soon affect its operations.

Just one year ago, our 2024 report on AI progress and issues suggested that despite remarkable acceleration in AI deployments, few organizations were positioned for long-term success. To delve more deeply into what's needed and deliver targeted and practical recommendations, our 2025 research explored the specific conditions and foundations required for AI success moving forward.

This report introduces an AI Readiness Index based on insights from our 2025 State of Application Strategy survey results as well as additional, targeted research conducted with 150 AI decision makers from organizations around the globe. They told us about their AI strategies, projects, supports, implementations, and concerns. The aggregate results inform a readiness index that captures the key elements of enterprise preparedness for the evolving demands of AI deployment.

Use the index and other information in this report to consider how your own organization stacks up against digital and AI leaders and to assess how best to avoid being left behind.



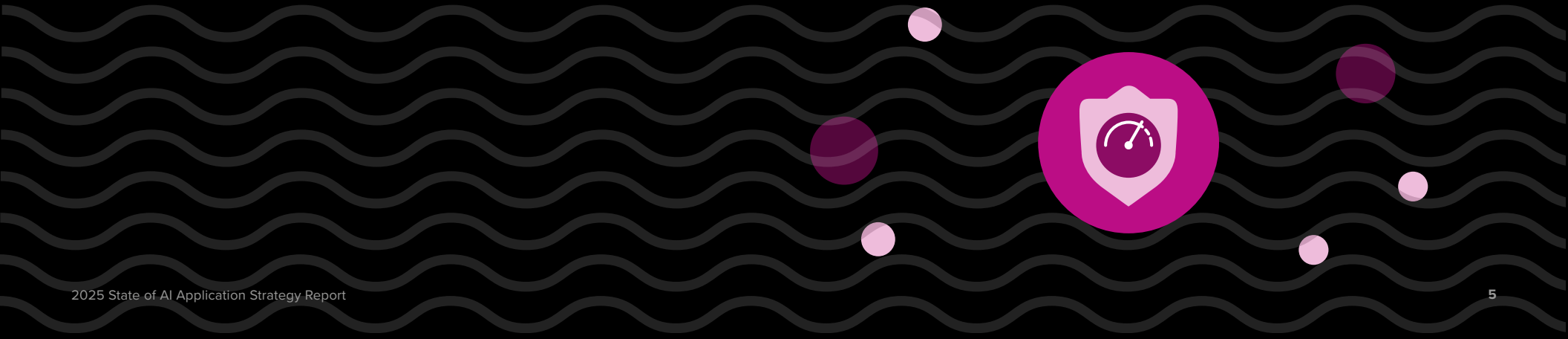
Methodology: Defining the AI Readiness Index

Unlike traditional IT maturity models, which typically focus on internal evolution of the organization, our AI Readiness Index quantifies *the operational capacity to successfully scale, secure, and sustain AI systems* across environments. It incorporates six measures explored in our 2025 research:

1. **Status of generative AI across five stages**—exploration, planning, piloting, deployment, and production.
2. **Adoption of AI agents across five stages**—exploration, planning, piloting, deployment, and production.
3. **Adoption of agentic AI across five stages**—exploration, planning, piloting, deployment, and production.
4. **Breadth of AI applications** as revealed by the number of different types of apps (such as chatbot, analytic, or personalization apps) into which AI is currently integrated.
5. **AI penetration** as measured by the percentage of organizational apps that use AI.
6. **Model diversity** as reflected in the number and variety of AI models deployed by the organization.

Results for each of these six factors were normalized and weighted to calculate a raw readiness score (from 0 to 5), and those scores were summed into a total readiness score from 0 to 30. That score was then scaled to a **Readiness Index** from 0 to 100, with organizations classified into three tiers:

- Highly ready organizations (indexes from 80–100) are actively deploying multiple types of AI with wide application, established AI model diversity, and strong integration indicators.
- Moderately ready organizations (indexes from 50–79) have implemented some AI with modest deployment scale and scope.
- Low-readiness organizations (indexes below 50) are still exploring or planning, may lack operational alignment, or are using AI only in limited ways.



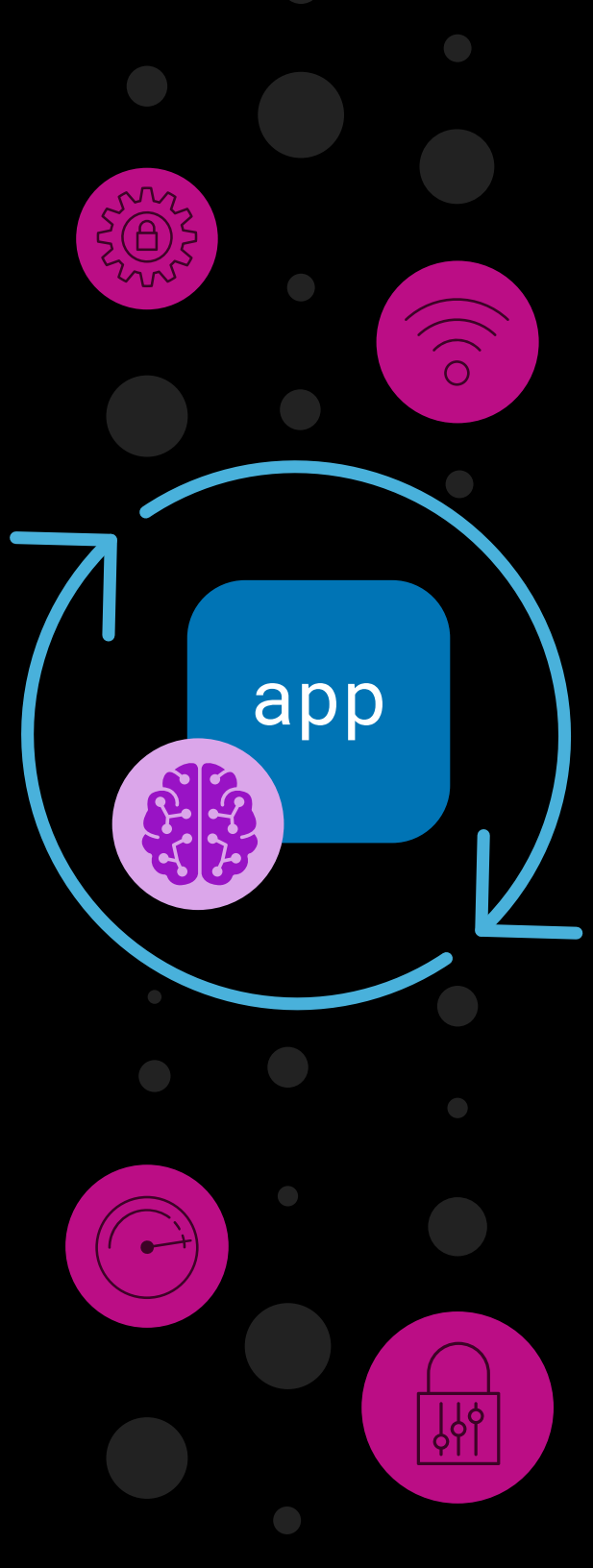
Key Findings: The 2025 AI Readiness Landscape

It will surprise no one that some industries, such as technology and financial services, are more ready for AI, and indeed further into implementation, than others. Similarly, since AI readiness generally tracks with digital sophistication, some regions of the world are farther ahead than others. What may be more startling is how decisions such as which AI models to use—or how many—can play a role in determining overall AI readiness.

Highlights from the 2025 research results include:

- Only 2% of respondents qualify as highly ready today.
- 100% of survey respondents use more than one AI model, making AI models as diverse as the multicloud environments most organizations rely on for app deployment.
  - 58% of the models in use by survey respondents are paid options (for example, Open AI's GPT-4), while 42% are open source (such as Mistral AI, Meta's Llama series, or Microsoft's Phi-2 or Phi-3).
- More than two-thirds of respondents (71%) say they've already augmented security using AI. Virtually everyone else plans to do so.
- While concern about third-party data misuse is high, it seems to prompt model diversification more than it affects model choice.

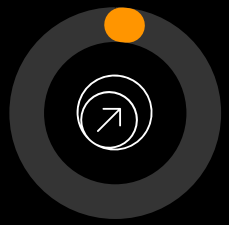
Keep reading for a detailed snapshot of highly ready and moderately ready organizations, an assessment of risks faced by organizations in a low-readiness state, and strategic recommendations for turning AI risks into opportunities by treating AI more like infrastructure—a platform for security, observability, growth, and innovation.



Section 1:

Who's Ready? Who's Not? Capabilities and Gaps

Overall, the organizations represented in our survey (all with annual revenues over $200 million and most with revenues between $500 million and $5 billion) earned readiness rankings that indicate a few are highly ready and the vast majority are moderately ready but one-fifth are not very ready at all.



2%
Highly ready

77%
Moderately ready

21%
Low readiness

This distribution reflects a landscape in which organizations are actively scaling AI operations while still struggling with significant governance, security, and infrastructure alignment issues.

70% of moderately ready organizations have generative AI in active use

For instance, 70% of moderately ready organizations have generative AI in active use, and more than half have deployed at least one AI agent. While they aren't yet saturating their application portfolios, AI is present in roughly one-third of their environments—comfortably above average, but not yet at scale. The top benefits cited include improved productivity, process efficiency, and customer experiences, though typically within isolated teams or workflows rather than in end-to-end operations.

However, these gains exist alongside persistent friction. Moderately ready companies are much more likely to struggle with cross-cloud policy inconsistencies, regulatory uncertainty, and infrastructure bottlenecks, particularly during model training. Security remains a central focus: Most surveyed organizations cite data protection, encryption, and prevention of prompt injection attacks as critical requirements, and a significant number are either using or planning to deploy AI firewalls and data processing units (DPUs).

Industries dominated by moderate readiness levels include financial services (81%), manufacturing (73%), and healthcare (74%), where legacy infrastructure is being steadily modernized, but at a cautious pace. By contrast, the government and education sectors remain heavily overrepresented in the low-readiness category, constrained by regulation and historical underinvestment.

Regionally, moderately ready organizations span both developed and emerging markets, with North America and Western Europe continuing to lead in adoption. Yet traction is increasing in the Asian Pacific and Middle East, regions where foundational cloud infrastructure is catching up quickly, even if full AI saturation remains a longer-term goal.

Hallmarks of Greater Readiness

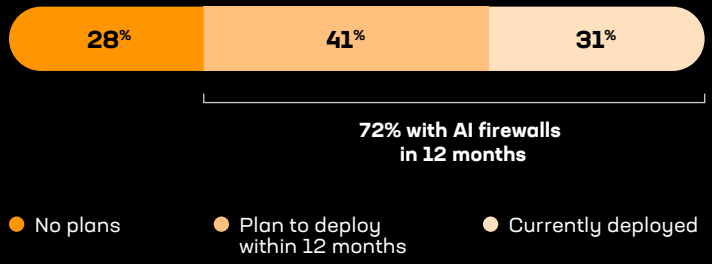
The factors that indicate high readiness in an organization, and therefore relative sophistication in AI use and ability to scale, include:

- The existence of formal data labeling practices (present in only 21% of moderately ready organizations).
- The use of AI across a wide variety of applications, from security and analytics to personalization for customers. Moderately ready organizations also excel here, using AI across five different types of applications, on average.
- Adoption of protective infrastructure like AI firewalls, a practice that is gaining ground. Nearly half (47%) of moderately ready organizations also have deployed or plan to deploy an AI firewall within the next year, though only 18% have already done so. This contrasts sharply with low-readiness organizations, where only 21% have deployment plans at all, and a mere 7% report having deployed such protections today.

Many high readiness organizations have formal data labeling practices

AI Firewall Deployment Status

Percent of all respondents (percentages rounded)



Embedded governance and big-picture strategies that embrace diversity across AI use cases, apps, and models are also key differentiators. Particularly striking is the number of models in use. Nearly two-thirds of survey respondents (65%) use two or more paid models and at least one open-source model. While a simple majority of models in use today are paid, open-source models are popular, too. The top ones in use by our survey population are Meta's Llama variants, Mistral AI variants, and Google's Gemma. The most common hybrid combination among the numerous permutations is GPT-4 or GPT-4 Turbo with a Mistral variant. Perhaps unsurprisingly, the use of multiple models like this correlates with deployment in more than one environment or location.

Interestingly, respondents using more paid models report higher confidence in governance, while those who work with more open-source models tend to have stronger data labeling practices—perhaps to mitigate perceived risks. Meanwhile, respondents are concerned about third-party misuse of data, but this concern doesn't seem to be reducing use of paid models from cloud hyperscalers. Instead, it encourages diversification of models more generally.

Moderately ready organizations are beginning to mature in how they approach data protection across AI workflows. Safeguarding sensitive customer information is a growing priority, but their methods tend to reflect evolving—not yet fully established—capabilities.

While some moderately ready organizations still rely on broad cloud security policies, many are starting to adopt more intentional techniques. Among them, 27% use inline enforcement across multiple layers. About 19% report federating control and applying tokenization, and 11% isolate data within infrastructure specific to the model in use.

The shift suggests a transitional phase—where awareness is high, but execution is still uneven.

Even organizations of moderate readiness are looking to AI for security. Nearly three-quarters of total respondents (71%) have already used AI to augment security. Another 27% plan to do so.

Capabilities of Highly Ready Organizations

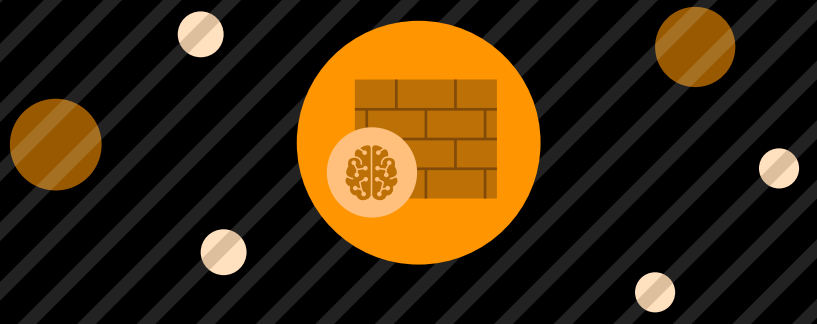
Moderately ready organizations are making real progress, but they haven't yet crossed into practices that define true AI maturity. To reach high readiness, more is required than isolated deployments or departmental use cases. High readiness means scale, diversity, and architectural integration across the organization.

Today's moderately ready organizations show momentum, however:

- **60%** use more than one type of AI model, typically a mix of paid and open-source options.
- **70%** have generative AI in production, a strong signal of practical adoption.
- **54%** have deployed AI agents, often in targeted domains like support or operations.

Only 35% are implementing agentic AI, though, highlighting a major gap in orchestration maturity. In addition, AI is present in about one-third of applications, far below the portfolio-wide saturation expected at high readiness.

To close the gap, moderately ready companies need to shift from tactical to strategic AI use—expanding model diversity, increasing application coverage, and embedding intelligent agents into the operational core. That's the difference between simply using AI and being ready to scale it.

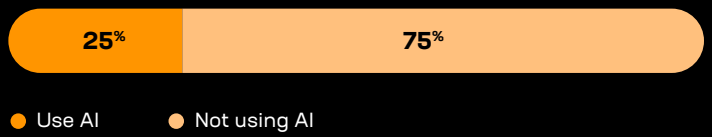


Low-readiness organizations may be exploring AI, but they haven't yet translated interest into operational capabilities. Most are still in the planning or pilot phase, with limited deployment and minimal integration. Their posture is cautious and often shaped by regulatory concerns, legacy infrastructure, or a lack of skilled resources.

These indicators show where low-readiness organizations currently stand:

- AI is used in fewer than 25% of applications (the overall average for all organizations), typically in siloed or experimental settings.
- Most use only one AI model, usually a single model from a paid provider.
- Few low-readiness organizations have begun implementing agentic AI or AI agents at scale.
- Just 36% have generative AI in production, compared to 70% among their moderately ready peers.

Percentage of Apps Using AI Today
Average percent across all respondents



The potential is there, with 68% of low-readiness organizations actively piloting or planning AI projects. But translating that activity into readiness requires investment, architectural alignment, and a shift from experimentation to execution. These organizations aren't behind because they're unaware—they're behind because they haven't yet built the operational muscle to support AI at scale.

Most low-readiness organizations use only one AI model

The Challenges for Those Falling Behind

Like any new technology in today's digital world, AI presents both opportunities and risks. Although frontrunners may make costly mistakes—and no organization is immune from the security, operational, and reputational risks of AI gone awry—those organizations currently operating with low readiness are more likely to struggle in the months and years ahead. Particular challenges revolve around:

- The integration of AI workflows.
- The adoption of AI use across multiple apps and application types.
- The development of AI model strategies that ensure both model diversity and security.

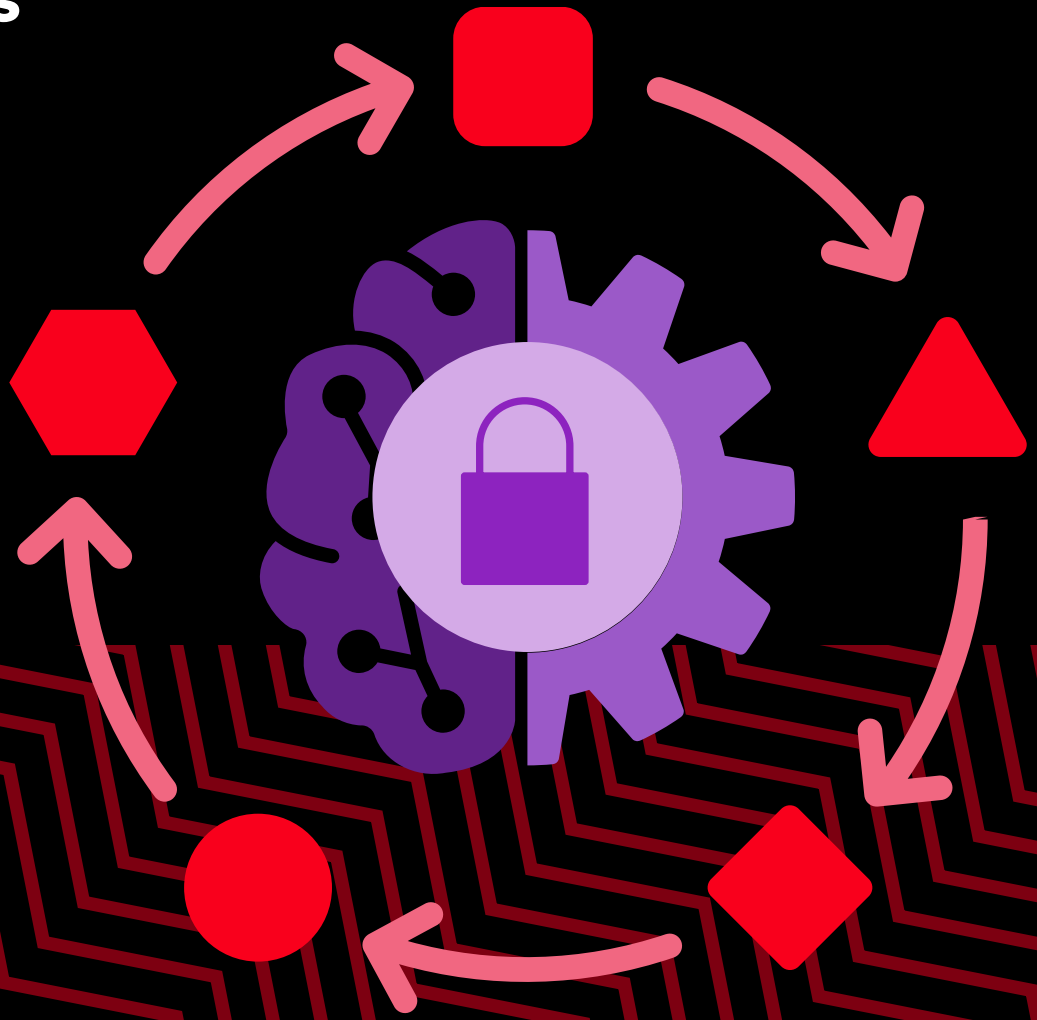
These gaps don't merely slow innovation—they expose the enterprise to risks related to governance, compliance, and workflow and app integration.

In addition, as AI accelerates it will drive corresponding leaps in the expectations of customers, management teams, shareholders, and regulators across industries. Even organizations in "traditional" or "high-touch" sectors will need to respond. How trailing organizations move to catch up will determine their long-term ability to efficiently serve customers and compete in an increasingly AI-modulated landscape.

Conversely, the organizations blazing the trail are ahead in more than deployment status. Indeed, they're more likely to treat AI as infrastructure rather than a feature, which enables better alignment of security, observability, and operational scale.

Section 2:

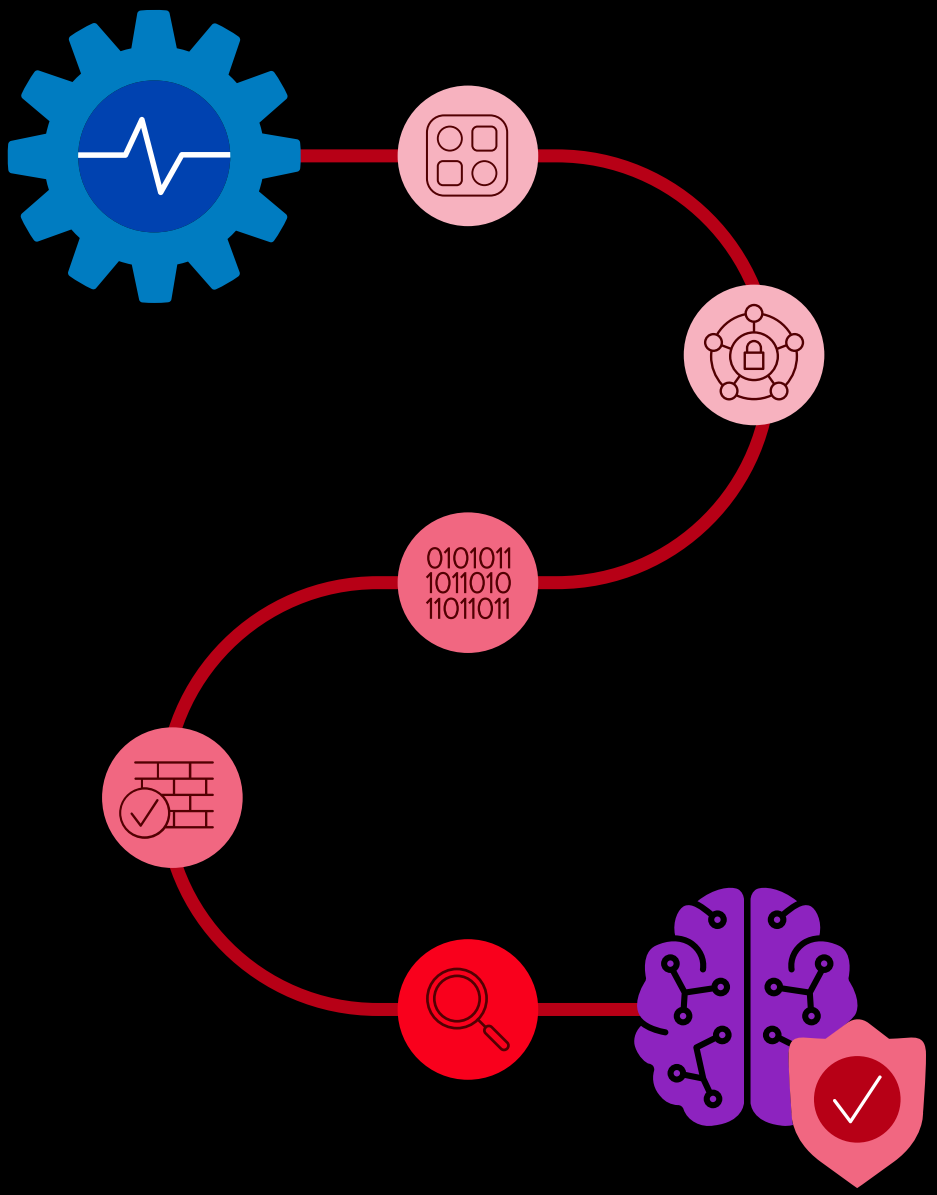
Strategic Recommendations



Organizations that find this data revealing can take these five steps to ensure they remain within sight of the leaders:

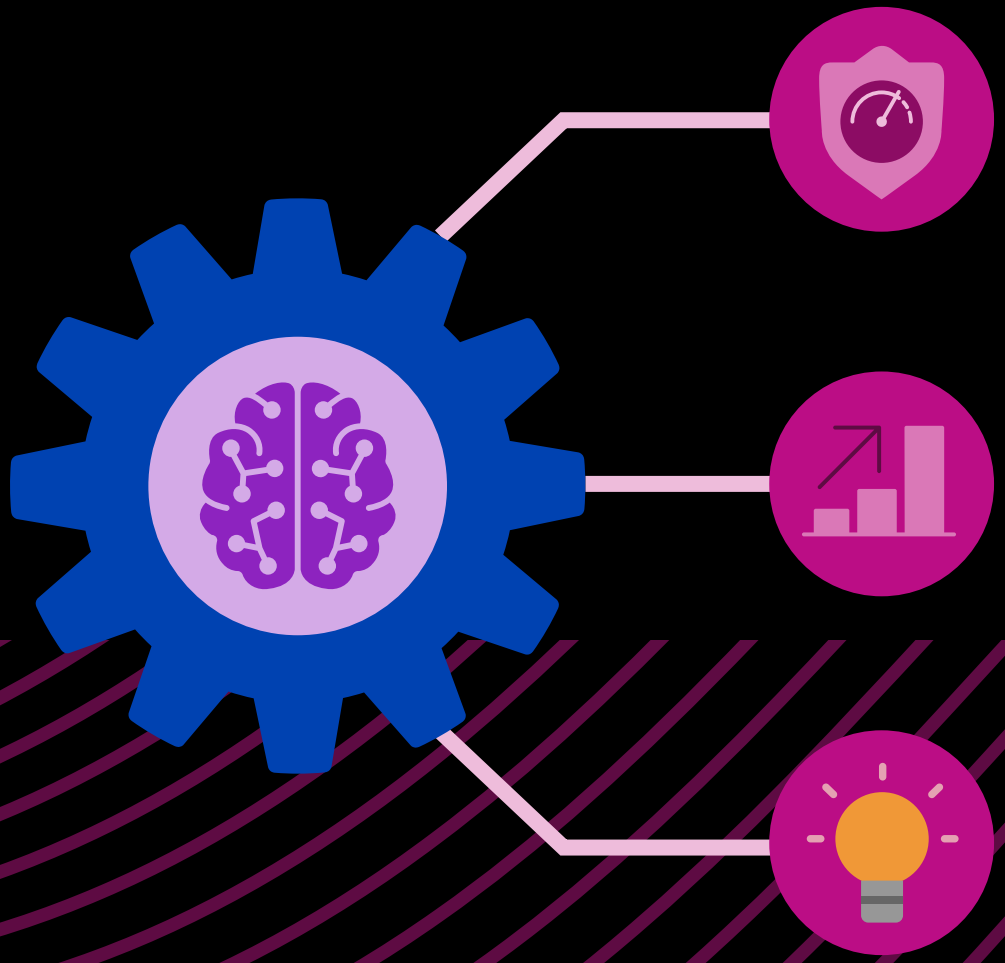
1. **Diversify model use.** Experiment with both open-source and paid AI models, and don't be afraid to use more than one of each for different purposes or use cases. Multiple models are likely the future for the same reasons most organizations rely on hybrid app deployment environments: Flexibility conquers most other considerations when balancing performance, security, and cost management.
2. **Expand AI across application types.** Don't constrain AI use to chatbots. Apply it to operations, security, analytics, and more to reap the benefits across functionalities and the business.
3. **Embed data labeling practices.** Basic governance measures such as data labeling are essential for transparency and AI risk mitigation.
4. **Align AI with security tooling.** From firewalls to observability and enforcement capabilities, AI can play a key role in protecting data, networks, customers, and the organization.
5. **Treat AI as a platform capability.** To unleash its full power, view AI as more than merely another tool in the box. Like infrastructure modernization or analytics, it's a comprehensive opportunity that should be broadly integrated into existing app and operational strategies.

View AI as more than merely another tool in the box



Conclusion:

Greater Orchestration Is Key

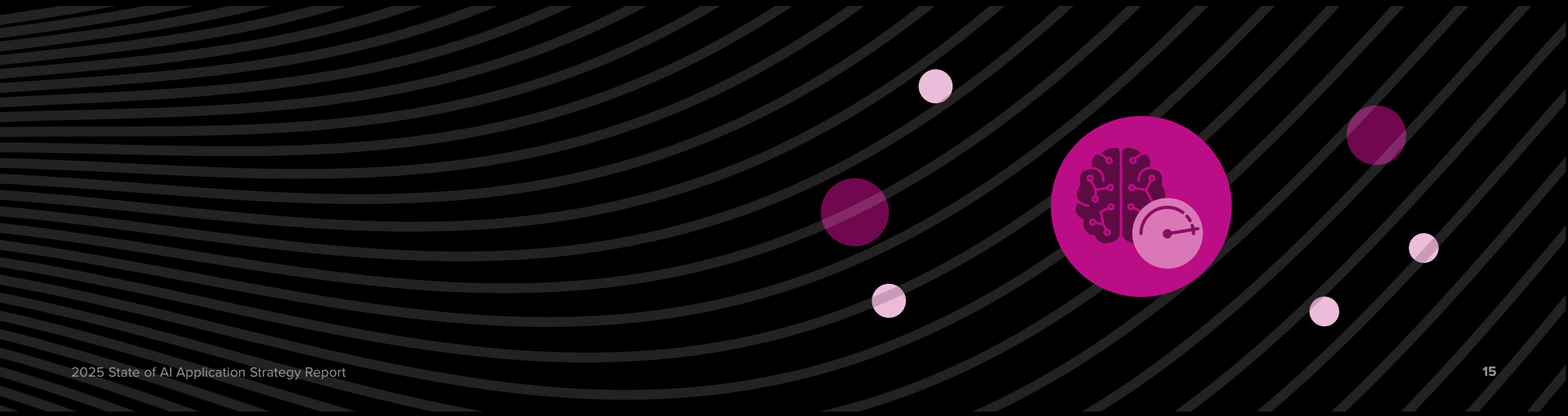


F5's 2025 research and the resulting AI Readiness Index show a clear division between early AI adopters and organizations with truly strategic AI alignment. Fortunately, most organizations making their way successfully through digital transformations and infrastructure modernizations already have the raw ingredients needed to assume a leading role in the AI revolution. The key additional steps to consider now are greater orchestration and prioritization, plus a cross-functional commitment to AI—not merely as a way to save time or money but as a core enabler of the business and its operations.

Those organizations that reach a high-readiness level—or already enjoy one—won't merely be more secure and more efficient. They will be more adaptive, more competitive, and better prepared to capitalize on whatever innovation comes next.

About this report

This report compiles data and analysis from both the eleventh annual F5 State of Application Strategy survey, which involved 650 IT decision makers across industries worldwide, and additional, in-depth research specifically on AI strategies. The targeted research engaged 150 decision makers with specific responsibility for their organizations' AI strategies and implementations. More than one-third were senior IT or business leaders, and 10 different industries across North America, Europe, and the Asian Pacific were represented. Only organizations with at least $200 million in annual revenues were included; more than one-third reported annual revenues of between $1 and $5 billion, and a significant percentage reported more than $10 billion.



ABOUT F5

F5, Inc. (NASDAQ: FFIV) is the global leader that delivers and secures every app. Backed by three decades of expertise, F5 has built the industry's premier platform—F5 Application Delivery and Security Platform (ADSP)—to deliver and secure every app, every API, anywhere: on-premises, in the cloud, at the edge, and across hybrid, multicloud environments. F5 is committed to innovating and partnering with the world's largest and most advanced organizations to deliver fast, available, and secure digital experiences. Together, we help each other thrive and bring a better digital world to life.