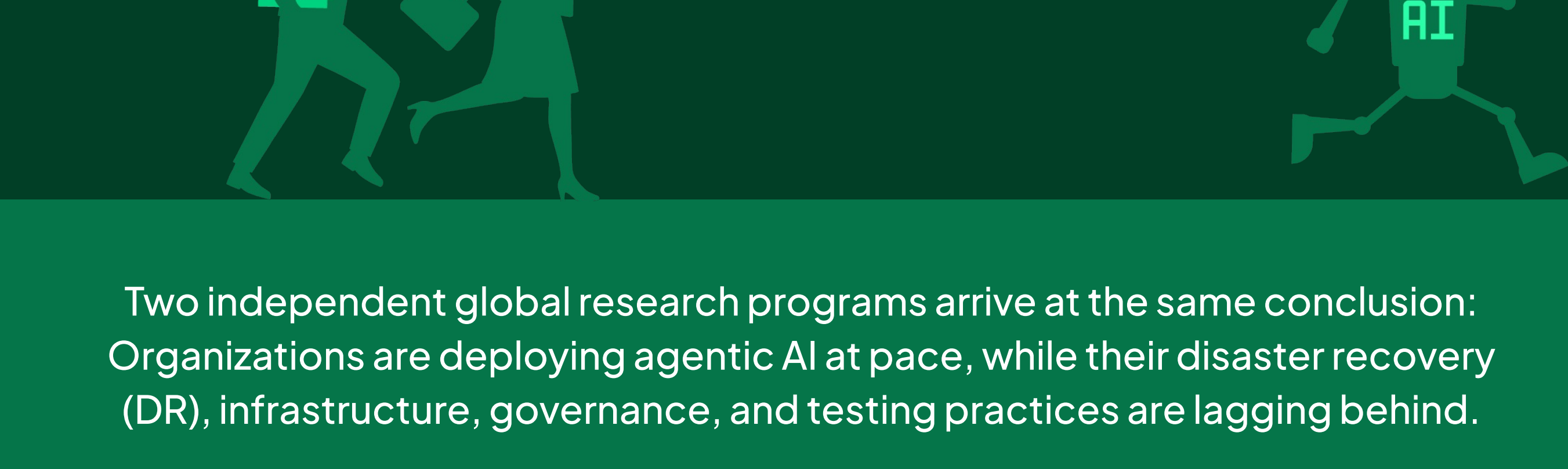


Agentic AI is moving fast. Is disaster recovery keeping up?

Many organizations believe their DR plans cover agentic AI. The data says readiness is often assumed — not tested.



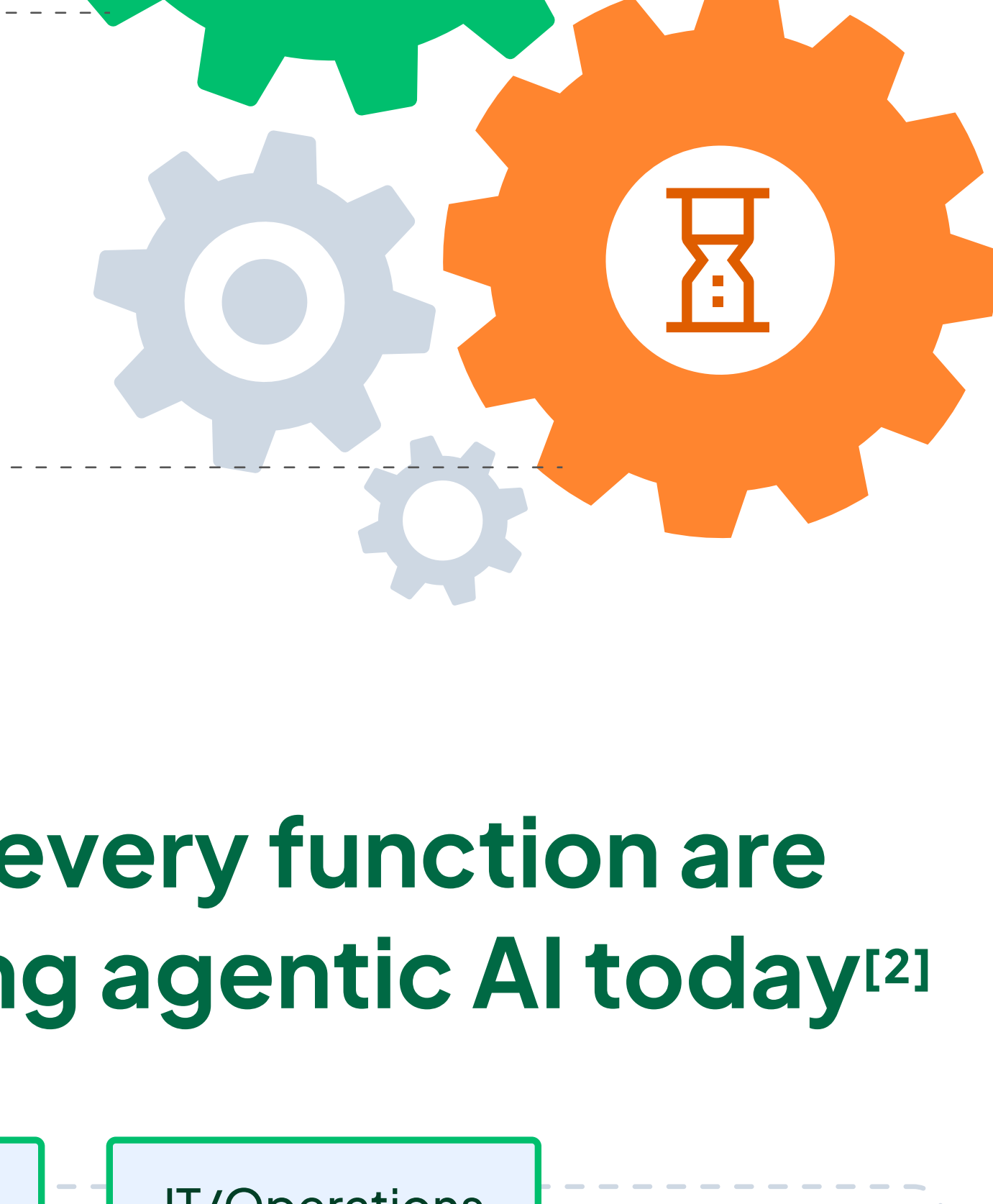
Two independent global research programs arrive at the same conclusion: Organizations are deploying agentic AI at pace, while their disaster recovery (DR), infrastructure, governance, and testing practices are lagging behind.

Both studies identify a gap between perceived readiness and proven, tested readiness. Confidence and capability are not the same thing — and the data suggests organizations have yet to close that distance.

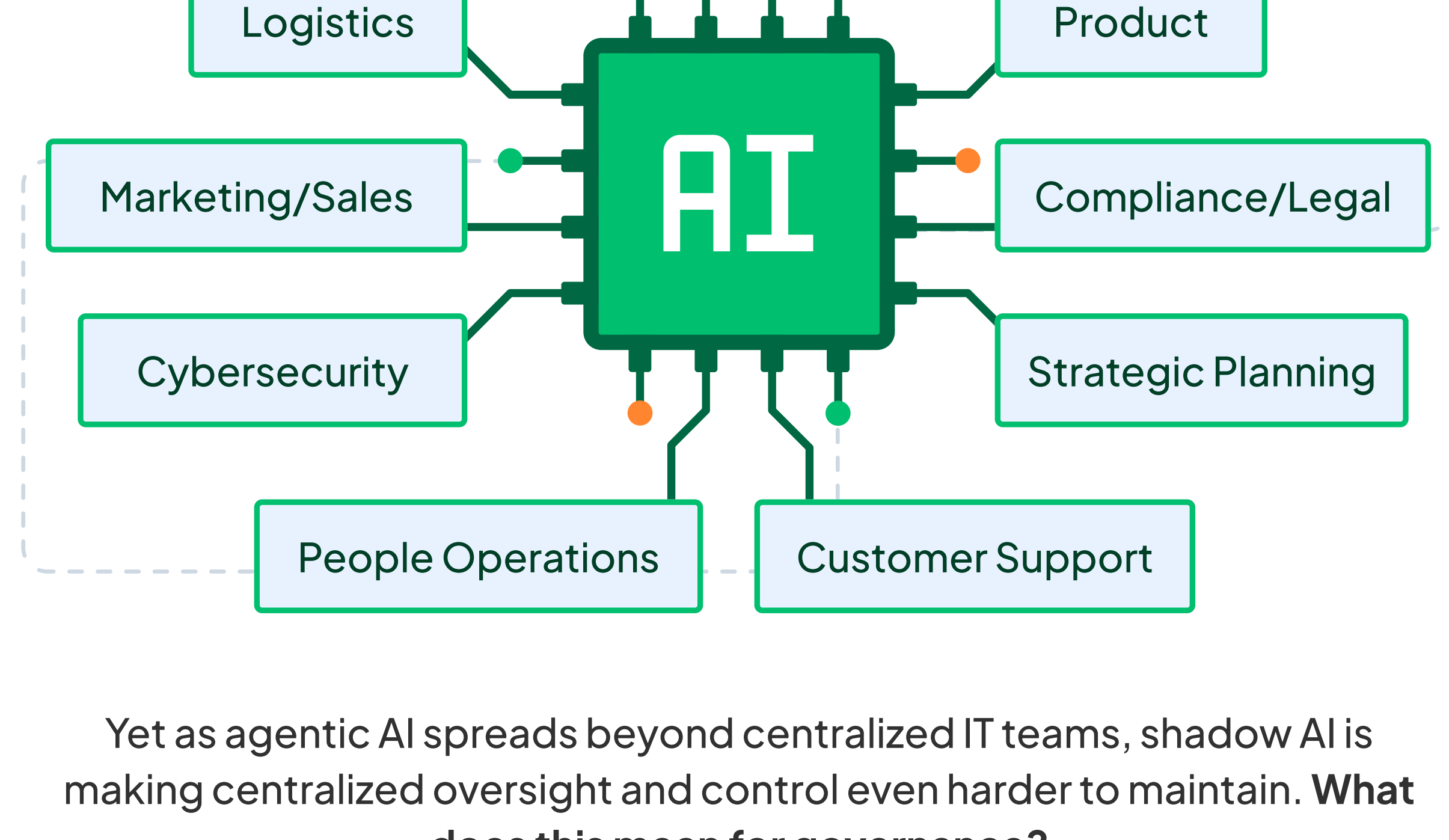
The state of AI adoption^[1]

53% of respondents report they have fully implemented agentic AI systems and tools across the organization.

47% of respondents are using AI in limited pilots or specific departments or are still in the planning phase.



Teams across every function are already deploying agentic AI today^[2]



Yet as agentic AI spreads beyond centralized IT teams, shadow AI is making centralized oversight and control even harder to maintain. **What does this mean for governance?**

Governance under pressure^[1]



67% of respondents believe their IT and security teams have full control and clear governance over the use of agentic AI in their organization.^[1]

33% of respondents report only partial or no control over the use of agentic AI in their organizations.^[1]

...Yet the same respondents name a lack of understanding of AI risk as their number one concern. *And you can't govern what you don't understand.*

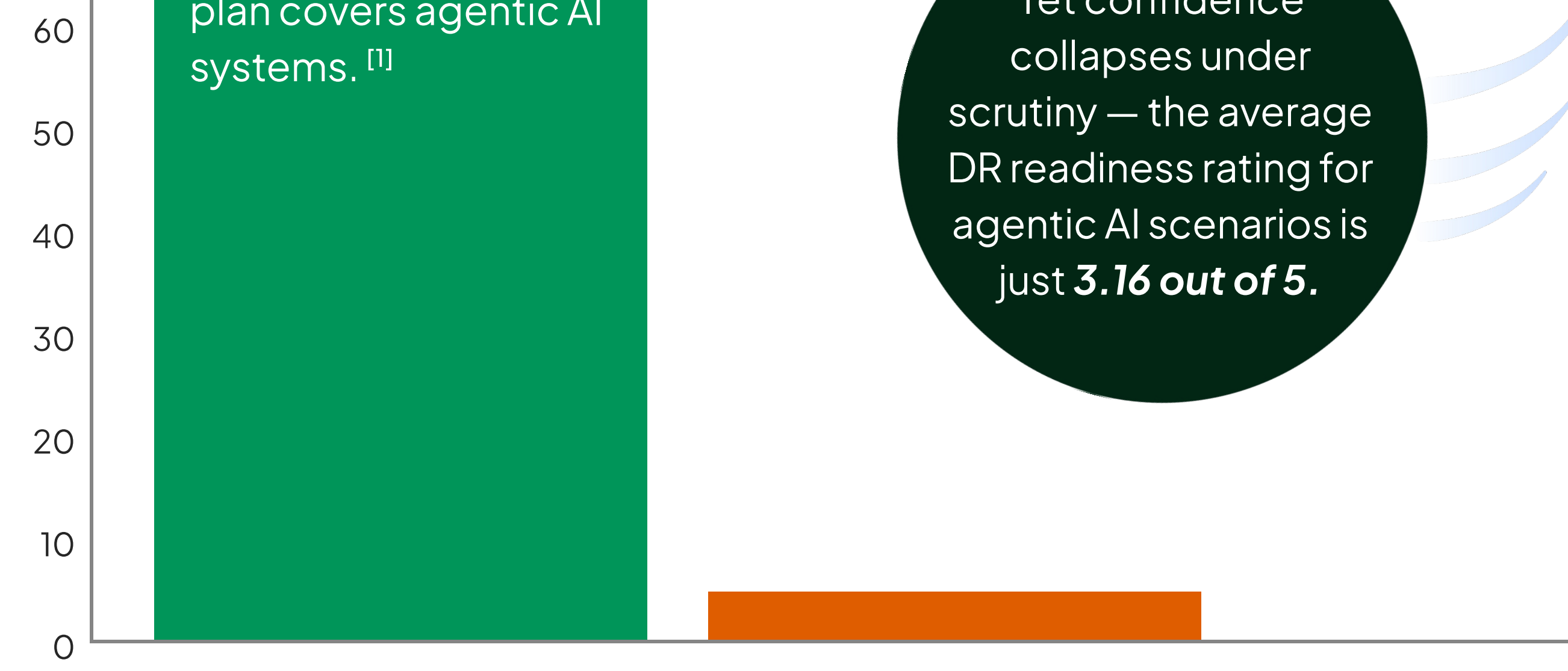
Top three concerns in agentic AI environments^[1]

1 Lack of understanding of AI risk

2 No ownership or accountability for AI systems

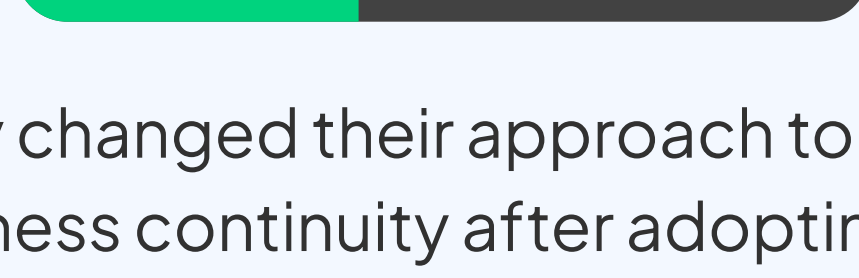
3 Low organizational awareness or priority

The disaster recovery gap^[1]



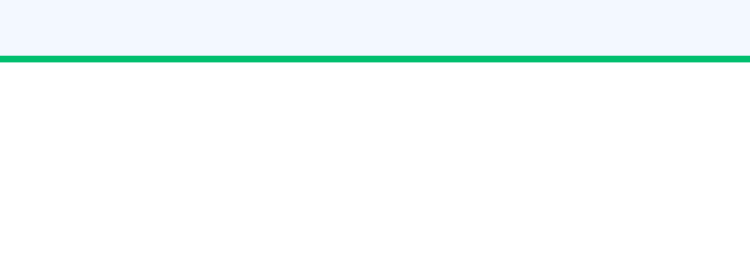
Yet confidence collapses under scrutiny — the average DR readiness rating for agentic AI scenarios is just **3.16 out of 5**.

Only 41% of respondents...



...have significantly changed their approach to data protection and business continuity after adopting AI.^[1]

And only 32% of respondents...



...test their DR plans monthly, the minimum cadence recommended for a dynamic AI environment.^[1]

“

In real-world recovery scenarios, **the problem is rarely the absence of backups.** It's knowing who is in charge of the recovery and which systems are restored first when multiple systems are affected.

 **Kim Larsen**
Group CISO at Keepit

”

Why the gap persists

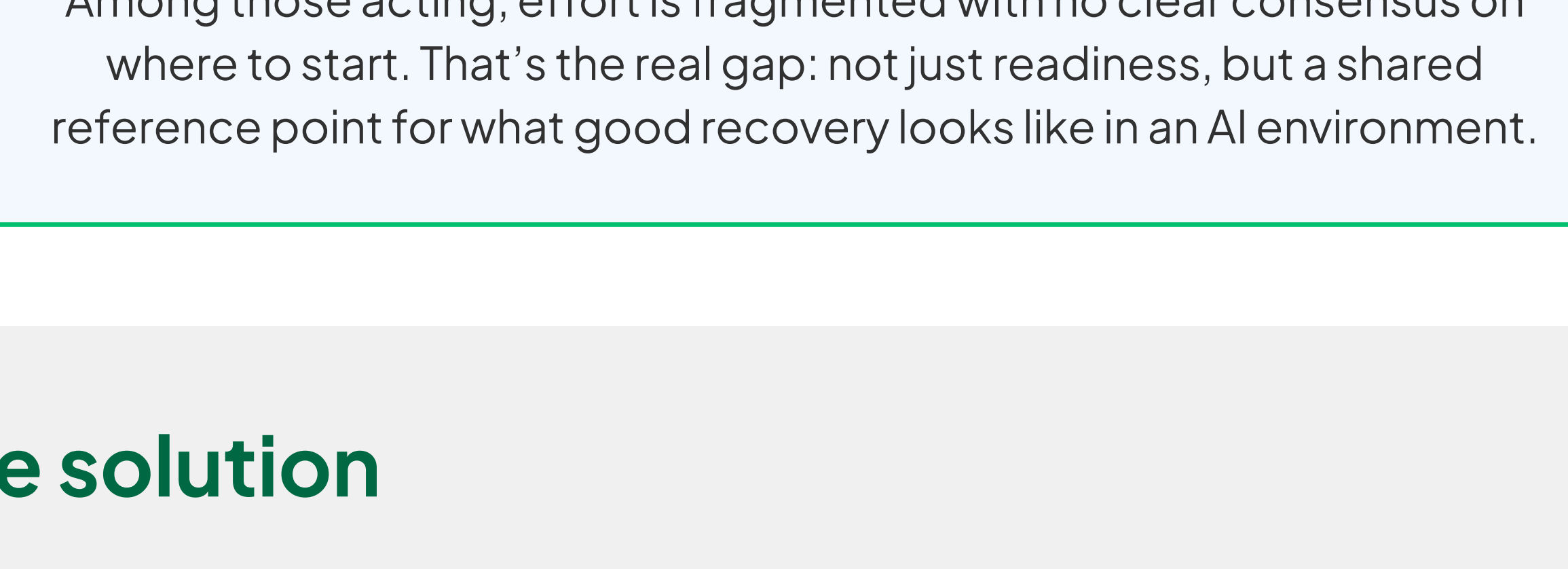
The top three DR barriers keeping leaders from closing the gap ^[1]



Next steps for DR modernization^[2]



Shockingly, 1 in 5 organizations plan to do *nothing*.^[2]



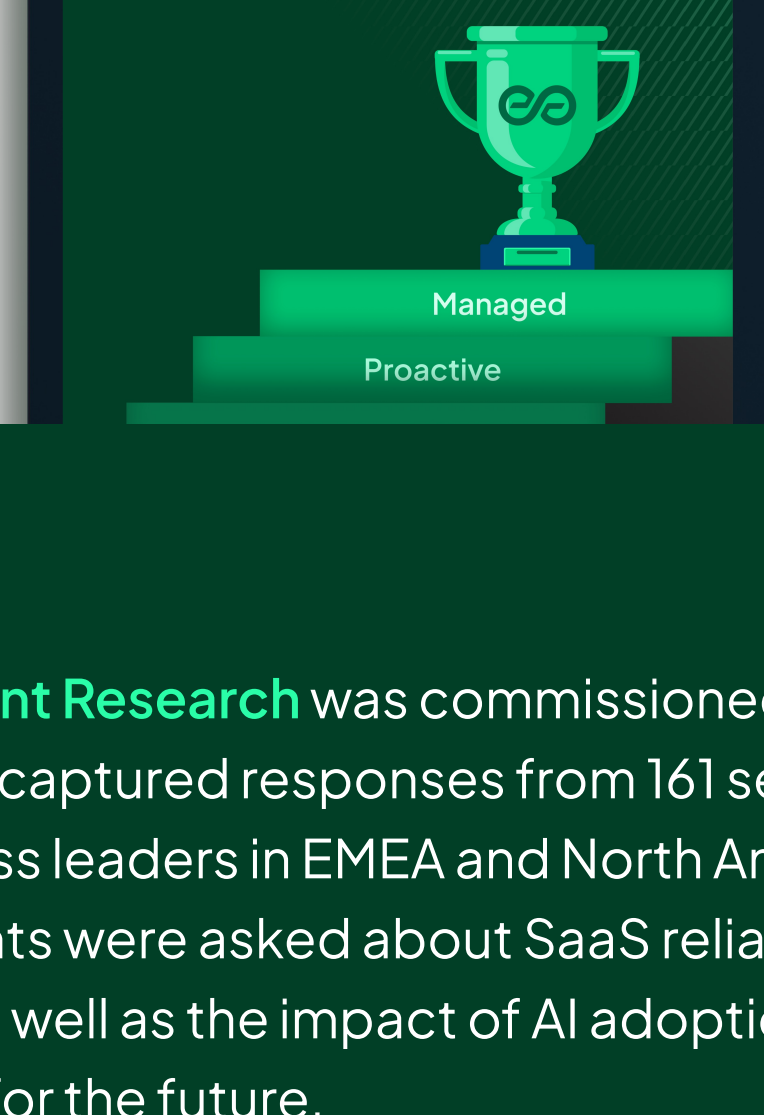
Among those acting, effort is fragmented with no clear consensus on where to start. That's the real gap: not just readiness, but a shared reference point for what good recovery looks like in an AI environment.

The solution

A structured maturity framework can give teams a common language and a prioritized plan for improvement. Understanding where your capabilities are today is the first step towards closing the disaster recovery gap.

Find out where you stand:
Assess your DR readiness now.

[Read the guide](#)



Sources

^[1] “**Peer insights on AI adoption and the disaster recovery gap**” is a report developed in partnership with CIO and based on insights of more than 300 senior IT decision-makers across the U.S., Europe, and APAC in global organizations with more than 1000 employees. Respondents were surveyed about how rapidly evolving AI environments are impacting disaster recovery (DR) strategies.

^[2] **Gatepoint Research** was commissioned by Keepit and captured responses from 161 senior IT and business leaders in EMEA and North America. Respondents were asked about SaaS reliance, DR maturity, as well as the impact of AI adoption and their plans for the future.