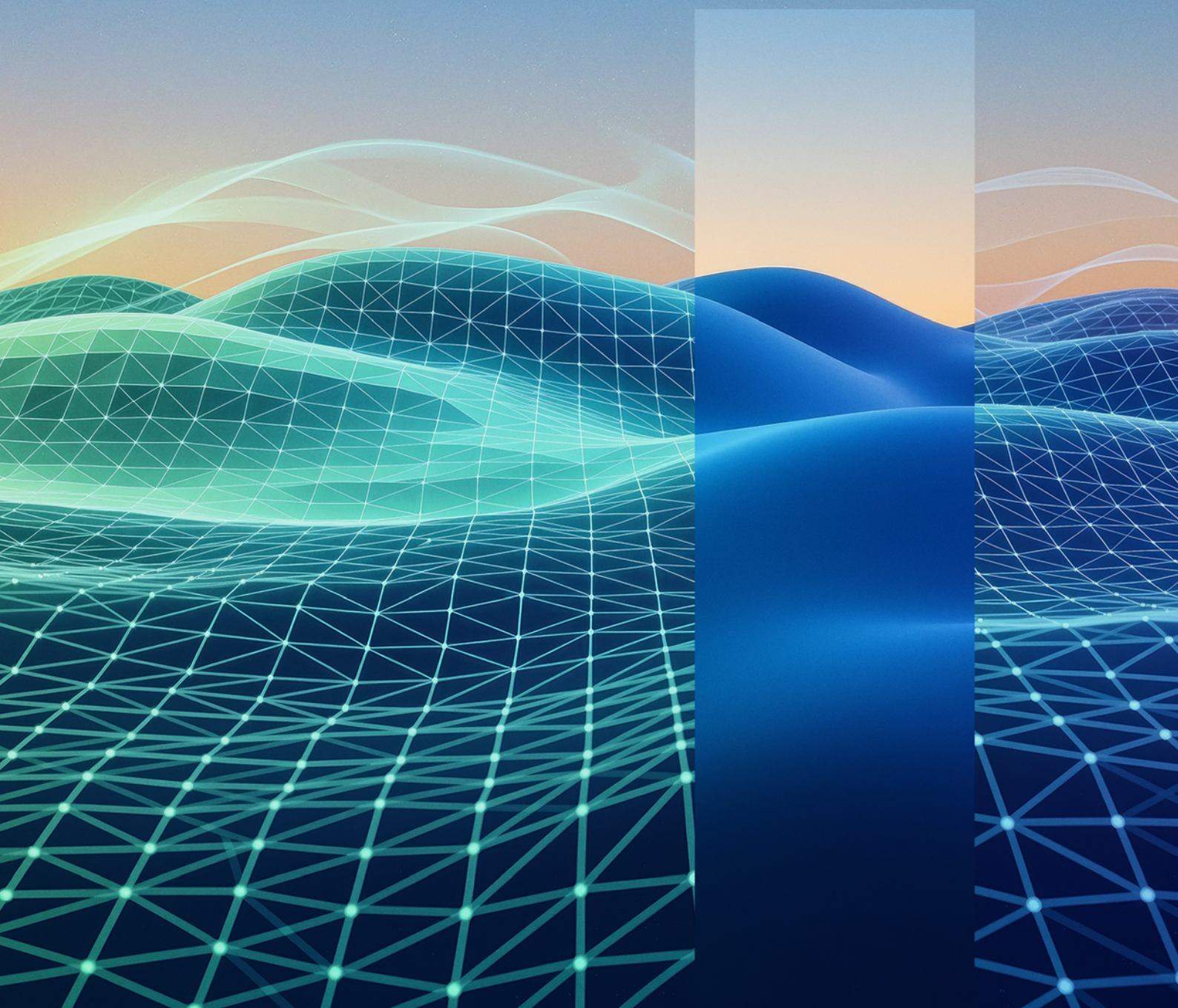
veeam Insights

Data Trust and Resilience

Executive Summary



Data Trust and Resilience: A Leadership Brief for 2026

Enterprise data has never moved faster or mattered more. At the same time, the systems that govern it are under unprecedented strain. Cloud platforms, automation, and AI have expanded the value of data and multiplied the ways it can be exposed, moved, or lost.

This brief draws on a global survey of more than 900 security leaders, including C-suite executives and frontline security teams.

Confidence is not proof

Most organizations believe they are prepared. In this research, 90% of respondents said they were very to extremely confident in their ability to recover from a cyber incident within defined recovery time objectives. Yet only 69% say those RTOs are fully aligned with business continuity goals. That gap often remains invisible until an incident exposes it.

Actual outcomes reinforce the concern. Among organizations that experienced a cyber incident in the past year, more than 40% reported customer disruption or financial loss. Nearly three in 10 experienced data loss, downtime, or business disruption. In ransomware incidents with operational impact or data encryption, full data recovery occurred in only 28% of cases.

Confidence rooted in policy and intent is not the same as recovery validated under pressure.

Agentic AI has changed the shape of data risk

AI is no longer experimental. It is embedded in everyday workflows and operates across applications, APIs, and third-party services. In the emerging agentic era, AI systems increasingly act on users' behalf by moving data and triggering actions with limited human oversight.

This shift fundamentally changes data risk. The attack surface expands. Governance requirements increase. The volume of data that must be protected and recovered grows with every new model, pipeline, and automated workflow. And visibility is not keeping pace.

Leaders report that this expansion is already outrunning their controls:

43%

say AI adoption is moving faster than their ability to secure data and models.

40%

have not updated security policies to address AI-specific risks.

42%

lack full visibility into the AI tools or models in use across the organization.

25%

cite unauthorized or shadow AI usage as a primary concern.

When organizations lack a clear view of where AI is in use, risk accumulates quietly and becomes visible only after an incident. In this environment, data trust can no longer be assumed. It must be built into how AI systems are governed, how data is protected, and how recovery is validated when disruption occurs.

Ownership without accountability

Many organizations have AI and data governance policies. Far fewer have translated them into enforceable controls. Fewer still have validated whether those controls hold under real-world pressure.

Responsibility typically rests with a single executive. 38% assign ownership to the CISO, while 27% assign it to the CIO. Only 17% report a cross-functional governance structure. Organizations with cross-functional policy committees were more likely to avoid a cyber incident altogether. AI and data risk span security, infrastructure, compliance, and business operations. No single role has full visibility across all of them.

Call to Action

The full Data Trust and Resilience Report 2026 examines where confidence breaks down, how AI governance gaps are emerging, and what differentiates organizations that recover cleanly from those that do not. Download the full report to explore the findings in depth