PRIMUS PARTNERS®

Sameer Jain, CEO, Primus Partners Solution

Published in Tech Circle
April 10, 2026

Reliable AI hinges on strong data security foundations

Authored by Sohni Bagchi

Read on: https://www.techcircle.in/2026/04/10/reliable-ai-hinges-on-strong-data-security-foundations

Article Content:

As enterprises accelerate the adoption of artificial intelligence (AI) across core business functions, a clear reality is emerging. Without robust data security, AI systems cannot deliver reliable or high-performing outcomes. Industry leaders say data integrity, governance and protection are no longer backend concerns—they sit at the heart of AI-led transformation.

“AI systems are only as trustworthy as the data they are trained on,” said Debojyoti Dutta, chief AI officer at Nutanix, in an interaction with TechCircle. “If the underlying data is compromised—whether through breaches, bias or poor governance—the outputs will reflect those flaws, often at scale.”

The shift comes as enterprises move beyond pilots to embed generative AI and agentic systems into mission-critical workflows. Across sectors—from financial services and healthcare to retail and manufacturing—AI is increasingly driving decision-making, automation and customer engagement. But the scale and sensitivity of enterprise data being fed into these systems is raising the stakes for security and compliance.

A key risk lies in the fragmentation of data ecosystems. As organisations pull in data from cloud platforms, legacy systems and third-party APIs, the attack surface expands. “Enterprises are dealing with highly distributed data environments,” said Prasanna Krishnan, head of collaboration and horizon at Snowflake. “Ensuring consistent security policies across these environments is complex, but essential for maintaining data integrity.”

At the same time, AI is introducing a new class of vulnerabilities. Data poisoning, model inversion attacks and prompt injection are emerging as material risks for organisations deploying large language models and AI agents—threats that can compromise sensitive data and distort outputs in ways that are often hard to detect.

“Security in the AI era is not just about protecting data at rest or in transit,” said Sameer Jain, CEO of Primus Partners Solutions. “It extends across the entire data lifecycle—from ingestion and training to inference and feedback loops.”

This is pushing enterprises to strengthen data governance frameworks, with a sharper focus on quality, lineage and accountability. Investments in tools that offer visibility into how data is sourced and used by AI systems are rising, particularly as regulatory scrutiny on data protection intensifies globally.

India is seeing a parallel surge in enterprise AI adoption, driven by its talent base and expanding digital infrastructure. But this growth is also bringing sharper focus on data privacy and responsible AI use. “India’s advantage in AI will depend on how effectively organisations balance innovation with responsible data practices,” Krishnan said.

The risks are compounded by what industry executives describe as growing “AI sprawl”. As enterprises deploy multiple AI tools and agents, concerns around fragmentation and rising technical debt are intensifying.

Vivek Ganesh, country head and regional vice-president for OutSystems India, said organisations risk ending up with hundreds of agents across platforms, complicating governance and security. “CIOs and CISOs are increasingly prioritising unified platforms that integrate application development, data systems and AI capabilities, rather than relying on fragmented tools,” he said.

Secure data sharing is another emerging challenge. As enterprises collaborate with partners and vendors, protecting sensitive information while enabling innovation is becoming a delicate balancing act. Technologies such as federated learning and privacy-enhancing computation are gaining traction as potential solutions.

“Enterprises need to rethink their data strategies from the ground up,” Ganesh said. “Security cannot be an afterthought—it has to be embedded into AI architecture from day one.”

The implications are significant. Weak data security can lead to regulatory penalties, reputational damage and flawed AI-driven decisions that directly affect revenue and customer trust. Conversely, organisations that prioritise secure, high-quality data are better positioned to scale AI reliably.

As AI becomes central to enterprise operations, the message from industry leaders is unambiguous: data security is not just a compliance requirement—it is the foundation on which effective AI systems are built.