CIO&LEADER

State of Enterprise Technology Survey

2025

Strategic Tech Signals and the CIO Action Agenda

In association with

bmnxt
business & market advisory

Contents

MANAGEMENT

Managing Director: **Dr Pramath Raj Sinha**
Printer & Publisher, CEO & Editorial Director (B2B Tech): **Vikas Gupta**
COO & Associate Publisher (B2B Tech): **Sachin Nandkishor Mhashilkar**

EDITORIAL

Group Editor: **R Giridhar**
Executive Editor: **Jatinder Singh**
Principal Correspondent: **Musharrat Shahin**
Correspondent: **Jagrati Rakheja**

CONSULTING ANALYST

Founder Analyst & Chief Research Officer, BM Nxt: **Deepak Kumar**

DESIGN

Creative Director: **Shokeen Saifi**
Assistant Manager- Graphic Designer: **Manish Kumar**

SALES & MARKETING

Director - B2B Tech: **Vandana Chauhan**
National Sales Head - B2B Tech: **Hafeez Shaikh**
Head - Brand & Strategy: **Rajiv Pathak**

COMMUNITY ENGAGEMENT & DEVELOPMENT

Head - Community Relations: **Dipanjan Mitra**
Head - Databases: **Neelam Adhangale**
Community Manager: **Vaishali Banerjee**
Community Manager: **Snehal Thosar**
Community Manager: **Reetu Pande**
Community Manager: **Nitika Karyet**
Assistant Manager - Community Development: **Shabana Shariff**

OPERATIONS

General Manager - Events & Conferences: **Himanshu Kumar**
Senior Manager - Digital Operations: **Jagdish Bhainsora**
Assistant Manager - Events & Conferences: **Sampath Kumar**
Video Editor: **Sunil Kumar**

PRODUCTION & LOGISTICS

Senior Manager - Operations: **Mahendra Kumar Singh**

Preface

The 2025 State of Enterprise Technology Survey captures the evolving priorities, challenges, and ambitions of India's top digital decision-makers. Based on insights from over 350 CIOs and technology leaders of India's top enterprises, the survey draws from both quantitative data and qualitative inputs collected between May and July 2025. It presents a shared understanding of the realities CIOs face today, as well as the strategies they are shaping for tomorrow. We hope these findings spark reflection, dialogue, and direction as you chart your enterprise technology roadmap.

At the heart of this year's findings is a clear message: Artificial Intelligence is no longer a distant promise—it is an enterprise imperative. As organizations seek gains in productivity, agility, cost optimization, and customer experience, AI is taking center stage. However, the ability to move beyond experimentation toward enterprise-wide impact remains a struggle for many.

While a small cohort of organizations is embedding AI into core processes and decision-making, the majority are navigating fragmented pilots, talent shortages, cultural resistance, or infrastructure gaps. The survey reveals that only 15.8% of enterprises are "Highly strategic and informed"—operationalizing AI at scale with governance, measurable outcomes, and organizational alignment. This relatively low figure highlights a gap between AI's perceived potential and its execution maturity.

At the other end of the spectrum, 7% of respondents report "Limited understanding," lacking awareness or preparedness for AI adoption. Between these poles, 26.3% are in an "Early-stage awareness" phase—recognizing AI's importance but not yet embedding it strategically—while 22.8% are "Moderately prepared," developing roadmaps and talent, yet facing uneven execution.

The survey also sheds light on critical adjacent priorities. Cybersecurity remains high on the CIO agenda, with 77% rating phishing attacks as highly or moderately severe—highlighting the persistent and evolving threat landscape. CIOs are responding by pushing for more intelligent, automated, and integrated security models.

Enterprise application modernization is another key area of focus. 76% of respondents cite refactoring legacy applications as a top priority—driven by the rise of microservices, DevOps, and container-native development. 58.6% highlight increased automation in software development and operations, while 50.7% emphasize enabling API-first development to drive modularity and integration.

Meanwhile, cloud adoption has matured. SaaS leads the way with 70% of enterprises using it in production, followed by 68% for IaaS and 58% for aPaaS. Security-as-a-Service (SECaaS) is also gaining traction, particularly in regulated sectors.

Taken together, the survey findings illustrate how Indian CIOs are reimagining the digital enterprise—progressing from technology adoption to business transformation, and ultimately toward building intelligent enterprises. We hope this report not only serves as a benchmark but also sparks deeper conversations and inspires bold decisions.

As you engage with these insights, we welcome your thoughts and reflections.

R. Giridhar
Group Editor
9.9 Group

Jatinder Singh
Executive Editor
CIO&Leader

Executive Summary

India's Enterprises Are Engineering An Intelligent Future

This year's State of Enterprise Technology survey reveals the pivotal role of trust, strategic orchestration, and precise execution in shaping India's next-generation digital enterprises.

In the golden age of scientific discovery, two inventions changed how we understood the world: the telescope and the microscope. One extended our vision outward—to the stars. The other inward—to the invisible. Today's enterprise leaders need both.

This edition of the State of Enterprise Technology captures the dual mandate. Indian CIOs and digital leaders are zooming in on security misconfigurations, app bottlenecks, and AI model bias. At the same time, they're looking ahead to cloud-native platforms, trusted AI ecosystems, and intelligent applications that respond in real time.

This isn't just digital transformation. It's strategic orchestration—where platform maturity meets cultural readiness, and data flows into decisions at scale. The telescope provides vision. The microscope delivers execution. Together, they define the intelligent enterprise.

Across AI, cloud, application development, security, and ecosystem strategy, this report distills what truly matters in 2025—not just the tools, but the thinking behind them. Welcome to the view from here—and what lies ahead.

The Big Picture Is in Focus

In 2025, Indian enterprises are visualizing digital transformation not as a sprint or a series of isolated upgrades—but as a long game of orchestration.

Leaders are thinking in systems, not silos. AI isn't an experiment. Cloud isn't just infrastructure. App modernization isn't a one-off initiative. Together, these elements form the strategic foundation of what many now call the intelligent enterprise.

The telescope is firmly in use: CIOs and business heads are aligning AI investments with growth, resilience, and innovation goals. Cloud strategies are no longer reactive—they're built around performance, interoperability, and AI readiness. Application development is shifting from project to product thinking, and data is being reimagined as a business asset, not just a technical input.

The result is a more confident, long-range mindset. Technology is no longer a toolkit—it's a lens for future-proofing the enterprise. And increasingly, it's the leadership vision—not just budgets or architectures—that will determine how far and how fast an organization can evolve.

Zooming Into What Matters

While the strategic view is expanding, 2025 also marks a turning point in execution discipline. Indian enterprises are no longer content with broad ambition—they're focusing on the nuts and bolts of transformation. The microscope is in steady use.

Modernization is now measured in milestones: containerized workloads, secure APIs, automated pipelines, and measurable app agility. AI isn't just being talked about—it's being embedded into IT operations, content creation, and decision systems. Identity and access management, once a compliance checkbox, is becoming a cornerstone of digital architecture.

Challenges remain: technical debt, data silos, cloud complexity, and the sheer pace of tool proliferation. But enterprises are responding with sharper integration strategies, deeper DevSecOps adoption, and more structured governance models. Success is no longer about who adopts first—it's about who scales intelligently.

The focus has shifted from 'what' technologies to 'howthey're implemented, secured, and sustained. It's clear: future-ready enterprises are built not just on vision, but on precision.

Trust: The Most Valuable Enterprise Currency
In the AI era, trust isn't a soft value—it's a hard requirement. As enterprises digitize faster, interconnect deeper, and automate more, their exposure widens. The 2025 survey makes it clear: security, privacy, and explainability have become foundational pillars—not just in IT, but in enterprise brand and resilience.

Enterprises are investing heavily in cloud security, zero-trust architectures, and identity governance. But they're also responding to a new layer of risk: AI-generated threats, model drift, and data misuse.

So, data privacy isn't just about regulation—it's about user confidence, cross-border compliance, and platform interoperability. The security posture is shifting from defensive to predictive, and from reactive to resilient.

Trust now travels across every API, model, and integration. The intelligent enterprise isn't just fast or scalable—it's accountable. In 2025, those who build trust by design will lead not just in adoption, but in influence and impact.

AI Is the New Enterprise Operating Layer
AI has evolved from a niche capability to a foundational layer of enterprise operations. In 2025, it powers everything from infrastructure resilience to customer experience, developer productivity to decision modeling. No longer confined to pilot zones, AI now runs in production—detecting, recommending, personalizing, and automating across functions.\Indian enterprises are embedding AI in IT monitoring, cybersecurity response, financial forecasting, and content generation. AI copilots are showing up in coding, CRM, and HR workflows. Just as cloud abstracted hardware, AI is abstracting complexity—turning insight into interface.

This shift isn't just about models—it's about maturity. Leaders are investing in governance frameworks, explainability, and internal build capabilities. They're rethinking KPIs, retraining teams, and integrating AI into enterprise architecture—not as a layer on top, but one beneath.

The intelligent enterprise is no longer defined by what it knows, but by how fast it can learn, adapt, and act. In 2025, AI isn't the future layer—it's the present logic.

From Silos to Systems: The Rise of the Connected Enterprise
In 2025, enterprise transformation isn't just about digitizing functions—it's about orchestrating ecosystems. Indian organizations are moving from siloed initiatives to systemic thinking, where cloud, security, data, applications, and AI don't just coexist—they coevolve.

APIs have become the nervous system of the enterprise, linking internal capabilities with partner platforms, customer touchpoints, and real-time intelligence. Low-code/no-code tools are enabling business users to shape their own digital workflows. Integration is no longer an afterthought—it's a design principle.

This shift is structural. Startups, hyperscalers, platform vendors, and internal teams now operate in shared, interdependent ecosystems. CIOs and CDOs are playing conductor—ensuring interoperability, trust, and shared outcomes across the value chain.

The connected enterprise isn't defined by any single product, platform, or provider. It's defined by how seamlessly intelligence flows across boundaries. In this model, scale is not a function of size—it's a function of coherence.

Study Overview

AI & Data Analytics: Scaling Intelligence, Embedding Insight

In 2025, Indian enterprises are no longer just experimenting with AI and analytics—they're scaling them across business functions. Compared to 2024's focus on data warehousing, governance, and integration, this year's survey highlights a decisive shift toward operationalizing AI, maturing data strategy components, and aligning initiatives with business outcomes.

AI usage is growing most rapidly in IT operations, cybersecurity, and customer experience, while adoption across finance, HR, and marketing shows expanding interest. Key goals now include real-time decision-making, operational agility, and cost optimization, with enterprises doubling down on AI-enabled automation and personalization.

Challenges persist, especially around data quality, change management, and selecting the right technologies, but are increasingly met with investments in AI literacy, cross-functional collaboration, and internal development capabilities.

Most notably, 93% of respondents expect to increase spending on AI and analytics, signaling strong executive confidence. In 2025, data is no longer just an asset—it's the foundation of adaptive, intelligent enterprise growth.

AI Ecosystem: Leadership, Strategy, and Signals of Scale

In 2025, Indian enterprises are evolving from AI adopters to AI orchestrators—focusing not just on implementation, but on governance, innovation, and vendor accountability. This year's survey goes beyond functional use cases to uncover how leadership readiness, strategic ownership, and partner ecosystems shape enterprise AI maturity.

AI strategy is no longer a siloed initiative—CIOs, business heads, and digital leaders are joint owners of the mandate, with growing clarity on goals like revenue growth, customer experience, and productivity. At the same time, solution selection is driven by explainability, scalability, and integration, not just performance benchmarks.

Enterprises are also deepening engagement with AI startups and innovation networks, while acknowledging the challenges of interoperability, talent access, and proof-of-concept validation. Leadership's AI readiness, ability to validate vendor claims, and openness to co-innovation now directly impact speed-to-scale.

From data to decisions, from ambition to accountability—the 2025 AI ecosystem is defined by intentionality, ecosystem design, and executive conviction.

Application Development: Modernizing for Speed, Intelligence, and Integration

In 2025, Indian enterprises are modernizing their application landscapes to meet the demands of agility, cloud nativity, and embedded intelligence. This segment highlights a decisive shift toward refactoring legacy apps, building cloud-native platforms, and aligning development with real-time business needs.

A majority of enterprises report strong adoption of microservices, DevOps, and containerization, while AI is being actively embedded into applications and workflows to improve automation, personalization, and insights.

App integration strategy is maturing, with APIs playing a central role in unlocking interoperability across environments. Meanwhile, low-code/no-code platforms are gaining enterprise trust, especially for internal productivity tools and departmental innovation.

The key success metrics have evolved—business alignment, developer agility, and time-to-market now matter as much as functionality or cost. Challenges remain, especially around managing technical debt, upskilling teams, and securing distributed architectures.

In 2025, the application stack is no longer static—it's dynamic, intelligent, and business-responsive by design.

Cloud & Infrastructure: Platform Maturity Meets Strategic Agility

The 2025 findings show Indian enterprises moving from broad cloud adoption to strategic cloud optimization. SaaS continues to dominate in maturity, but IaaS and emerging models like aPaaS and SECaaS are gaining ground—considered not just for cost or availability, but for performance, innovation, and ecosystem alignment.

Application hosting strategies now reflect a more nuanced hybrid approach: public cloud leads for office productivity and customer-facing workloads, while mission-critical systems and data resilience functions remain anchored in private or hybrid models. AI and analytics workloads are prompting a re-evaluation of infrastructure readiness, especially around data pipelines and model acceleration.

The top motivators for continued cloud investment—business agility, modernization, and innovation—remain unchanged. However, enterprises now pair these with operational KPIs and AI-readiness metrics. Security concerns persist, especially around configuration control, multi-cloud visibility, and open-source risks.

In 2025, cloud is no longer just infrastructure—it's the operating fabric of the intelligent enterprise.

IT Security: Evolving from Threat Response to Intelligent Resilience

The 2025 SET survey reveals how Indian enterprises are moving beyond perimeter defense toward intelligent, adaptive security frameworks. Compared to 2024—when phishing (50%), identity-based attacks (44%), and ransomware (38%) dominated concerns—the focus has shifted to managing complexity, scaling automation, and integrating AI.

The most severe impacts of security incidents—business disruptions, data loss, and financial damage—remain persistent, but enterprises are responding with greater strategic depth. In 2024, top responses included employee training (69%) and re-skilling IT teams (64%). In 2025, those measures continue, but are now complemented by cloud-native controls, PAM, SOCs, and privacy automation.

AI is both a tool and a target—driving detection capabilities while raising new risks like model poisoning and data leakage. The shift is clear: from reactive to proactive, from compliance to capability. This segment captures how CIOs and CISOs are reframing security as a driver of trust, agility, and digital confidence.

AI & Data

Operationalizing Intelligence at Scale

Indian enterprises are embedding AI and analytics deeper into their processes, platforms, and decisions—shifting from experimental pilots to measurable, organization-wide outcomes.

Contents

Executive Summary

In 2025, AI and analytics are no longer aspirational—they're operational. Indian enterprises are using these technologies to drive better decisions, improve efficiency, and gain a competitive edge. A full 100% of respondents cite decision-making through insights as a top priority, followed by cost optimization (98.4%) and business agility (98.4%).

Adoption is most mature in IT operations, customer service, and finance, with over 40% of enterprises reporting broad deployment of AI in these areas. AI is now embedded in incident response, network management, and even content generation—transforming both backend workflows and customer-facing experiences.

To support this momentum, enterprises are also strengthening their data strategy foundations. Components like data analytics & usage, data planning, and engineering pipelines score the highest in maturity, while governance and culture are still catching up.

Challenges persist. 90% of respondents cite data quality issues, and 86% highlight change management as a barrier to scaled deployment. Choosing the right tools and addressing privacy and model transparency are also front-of-mind.

Nevertheless, confidence is strong: 93.5% of enterprises plan to increase their AI and analytics spending, with over half projecting significant increases. Internal development is the preferred route for acquiring AI capabilities, but AI-as-a-Service and strategic partnerships also play important roles.

As enterprises move from dashboarding to embedded intelligence, AI is fast becoming a core operating layer. The focus now: govern well, deploy fast, and scale responsibly.

DATA DELUGE: TEXT, IMAGES, AND VIDEO DOMINATE THE GROWTH CURVE

Enterprise data landscapes are shifting rapidly, driven by collaboration platforms, digital experience tools, and AI-first operations. The 2025 SoT survey reveals that the fastest-growing types of data are unstructured—especially text, images, and media files. This has major implications for how organizations store, process, and analyze data in the AI era.

We're no longer just collecting data—we're generating streams of language, visuals, and interactions.

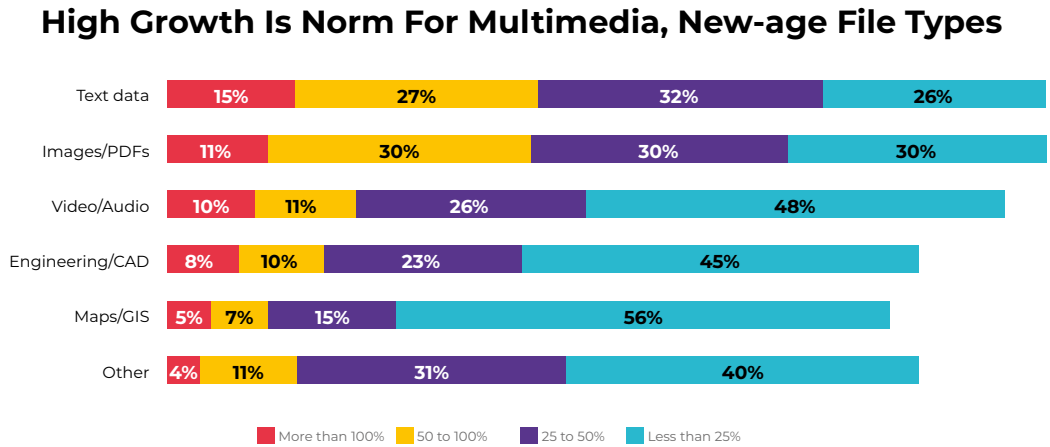

Figure 1: Unstructured formats—especially text and media—are expanding fastest, reshaping analytics and storage priorities.

Which Data Types Are Growing Fastest?

Based on respondents reporting data types growing at 25% or more annually:

- **Text data tops the list,** with 74.2% of respondents reporting high growth.
- **Image and PDF data follows closely at 70.5%,** driven by mobile uploads, scanned documents, and AI vision use cases.
- **Video and audio formats show 47.6% growth,** reflecting rising use of recordings, calls, and streaming content.
- **Engineering/CAD and Other data types** show more moderate growth, under 46% in the ≥25% range.

These findings reflect the **explosive growth of unstructured data,** compared to slower-growing structured enterprise data like logs or forms.

What the Growth Trends Tell Us

- **Unstructured Is Now the Norm**
  As enterprises digitize customer service, field operations, and employee engagement, text,

images, and audio become the new data backbone.

- **AI and Automation Fuel the Spike**
  Document digitization, OCR, NLP, and computer vision use cases are driving organizations to collect and store more rich media data..
- **Search, Security, and Storage Must Adapt**
  Traditional databases and security models are insufficient—unstructured data demands advanced indexing, vector search, and contextual controls.
- **Not All Data Types Are Equal in Growth or Readiness**
  Some formats like CAD files grow more slowly—but require high fidelity and specialized handling.

> "100% of enterprises say better decision-making is the top goal of AI—insight is no longer optional, it's integral."

CIO Action Agenda

- Reassess data lake and warehouse architectures to accommodate high-volume, variable-format data.
- Deploy tools for parsing, labeling, and securing text, image, and video inputs—especially in regulated environments.
- Align AI models with actual data growth—invest in pre-processing and enrichment pipelines for unstructured inputs.
- Reevaluate storage tiers and retrieval models to optimize for cost, speed, and accessibility

Key Insight

The future of enterprise data is not neatly structured—it's sprawling, sensory, and semi-formal. CIOs and CDOs must shift from tabular thinking to multimodal strategy.

Takeaways for Ecosystem Partners

- **Data platform providers** must support native handling of text, image, and audio—integrated with AI and vector indexing.
- **Cloud vendors** should offer cost-effective, AI-ready storage tiers for dynamic and diverse unstructured formats.
- **AI/analytics toolmakers** need to address upstream ingestion, labeling, and classification of non-tabular data.

Bottom Line

Your biggest data opportunity—and your biggest analytics blind spot—may be hiding in plain sight: emails, PDFs, chats, images, and recordings. Enterprises that master unstructured data will lead the next wave of intelligence and insight.

DATA STRATEGY MATURITY: ANALYTICS LEADS, CULTURE AND GOVERNANCE STILL GROWING

The effectiveness of AI and analytics hinges on the maturity of the underlying data strategy. The 2025 SoT survey reveals that while Indian enterprises have made solid progress in areas like analytics usage and strategic planning, critical enablers like data culture, governance, and engineering are still catching up.

Data maturity is uneven—strong in insights, but still developing in operations and accountability.

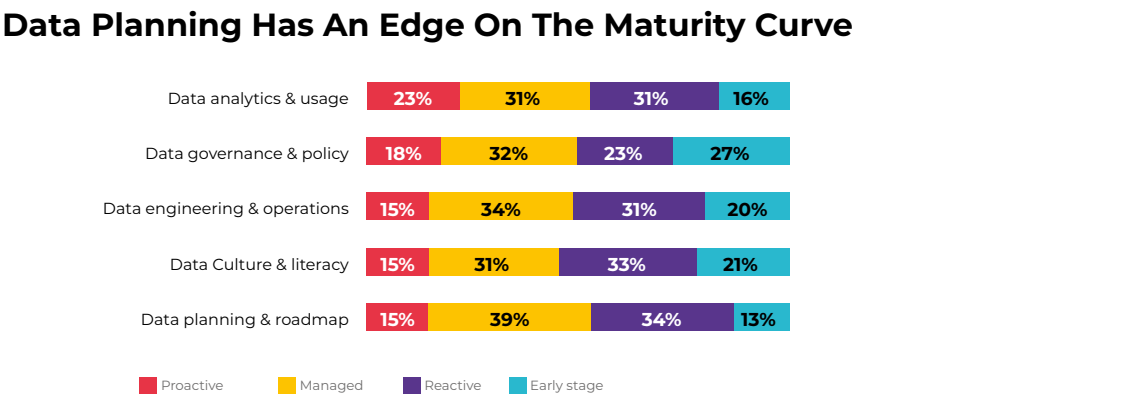

Figure 2: Data usage and planning show the highest maturity—culture, governance, and engineering trail slightly behind.

Which Data Strategy Components Are Most Mature?

Based on a weighted score that reflects progress from early stage to proactive maturity, the top-ranking components are:

- **Data analytics & usage ranks highest with** a maturity score of 2.60. Nearly 53% of respondents rate their analytics practice as managed or proactive.
- **Data planning & roadmap follows closely at 2.55,** showing strong commitment to aligning data with business needs.
- **Data engineering & operations** scores 2.44—signaling a solid foundation but with room to scale and automate.
- **Data governance & policy (2.40)** and **Data culture & literacy (2.39)** rank lowest—despite being essential to long-term data trust and effectiveness.

This pattern highlights that while enterprises are doing more with data, many are still building the capabilities to manage and scale how data is created, shared, and used.

What These Maturity Levels Tell Us

- **Analytics Is Where the Value Is Seen**
  Enterprises continue to prioritize dashboards, insights, and business-facing use cases—making analytics the most advanced function.

- **Strategy and Planning Are Gaining Discipline** Many organizations now have structured roadmaps and data investment frameworks—often tied to digital transformation.
- **Engineering and Governance Are Table Stakes—but Still Maturing** Pipelines, quality, access control, and lifecycle management remain pain points as data volumes and diversity expand.
- **Culture Is the Missing Link** Data literacy, democratization, and behavioral change are lagging—potentially limiting the impact of even advanced tooling.

93.5% plan to increase AI and analytics spending, with over half projecting significant growth—confidence in value creation is high.

CIO Action Agenda

- Strengthen governance frameworks with enforceable policies, automated controls, and cross-functional ownership.
- Invest in data literacy programs—tailored by function and embedded into everyday workflows.
- Scale engineering efforts through automation, reusable data products, and low-code tooling.
- Review and refresh the data strategy roadmap annually—aligning it with business changes and regulatory shifts.

Key Insight

Enterprises are eager to use data—but not all are ready to govern it. Without culture, governance, and engineering maturity, analytics success remains fragile.

Takeaways for Ecosystem Partners

- **Data platform vendors** must provide end-to-end tooling that supports ingestion, quality, cataloging, and stewardship.
- **Advisors and integrators** can help map maturity gaps and develop pragmatic roadmaps tied to business priorities.
- **Training partners** should focus on role-specific data enablement—not generic workshops.

Bottom Line

Your biggest data opportunity—and your biggest analytics blind spot—may be hiding in plain sight: emails, PDFs, chats, images, and recordings. Enterprises that master unstructured data will lead the next wave of intelligence and insight.

WHAT AI IS REALLY FOR: EFFICIENCY, RESILIENCE, AND SMARTER DECISIONS

The promise of AI and data analytics is often framed around breakthrough innovation. But the 2025 SoT survey tells a more grounded story: Indian enterprises are investing in AI to boost operational agility, streamline decisions, and sharpen their competitive edge. Goals like better insights, cost efficiency, and adaptability rank higher than more aspirational outcomes like ESG transformation or workforce disruption.

AI is not just an R&D initiative—it's a business performance lever.

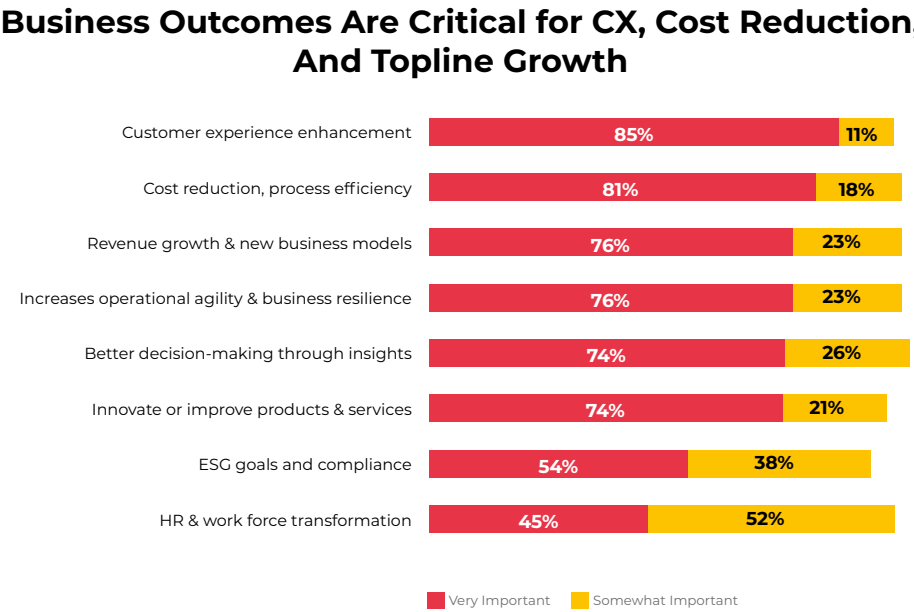

Figure 3: Enterprises prioritize decision support, cost savings, and agility over moonshot innovations.

Top Business Goals Driving AI & Analytics Initiatives

Survey respondents rated the importance of specific outcomes for their AI and analytics programs. Ranked by combined "Very Important" and "Somewhat Important" responses, here's what stood out:

- **Better decision-making through insights** topped the list with 100% combined importance—showing AI's role as a cognitive enabler.
- **Cost reduction and process efficiency** was rated highly by 98.4% of respondents, including over 80% who marked it "very important."

- **Operational agility and business resilience (98.4%) and Revenue growth or new business models (98.4%)** were also top-tier priorities.
- **HR & workforce transformation,** while still important (96.8%), was ranked lowest among the five—suggesting it may be more difficult to achieve or less of a current focus.

This pattern highlights that while enterprises are doing more with data, many are still building the capabilities to manage and scale how data is created, shared, and used.

Interpreting the Outcome Hierarchy

- **Insights Over Intuition** Enterprises see AI as a decision-support layer—augmenting judgment with patterns, forecasts, and real-time clarity.
- **Efficiency is a Core Business Case** Especially in cost-sensitive sectors, automation and optimization are clear, measurable wins.
- **Adaptability and Growth Go Hand-in-Hand** Agility, resilience, and innovation are not competing goals—they're sequential. AI helps enterprises respond faster and scale smarter.
- **People-Centric Outcomes Are Still Emerging** HR transformation is often constrained by cultural readiness, regulatory complexity, and fragmented data.

> Enterprises are using more data than ever, but many still lack the muscle to manage, scale, and govern how it's created, shared, and used.

CIO Action Agenda

- Anchor AI use cases to clear business KPIs—especially decision speed, accuracy, and process throughput.
- Prioritize projects with measurable impact—cost savings, revenue growth, or cycle time reduction.
- Partner with operations, finance, and marketing to identify areas where AI can unlock both efficiency and innovation.
- Begin HR and ESG-focused initiatives with pilots and stakeholder workshops—these often requires more cultural change than technical enablement.

Key Insight

AI's greatest impact today lies not in radical disruption—but in repeatable, scalable improvements to how businesses operate and decide. Enterprises that align AI to operational and strategic priorities will gain traction faster than those chasing futuristic visions.

Takeaways for Ecosystem Partners

- **Platform providers** should emphasize business-ready applications—dashboards, copilots, and optimization tools with quick ROI.
- **Service providers and consultants** can add value by aligning AI pilots to cross-functional pain points—not just data science ambition.
- **Tool vendors** must integrate analytics into decision workflows—not just visualization layers.

Bottom Line

The AI payoff is practical. CIOs who focus on decisions, efficiency, and agility—not just buzzwords—will turn insight into impact faster than their peers.

AI ACROSS THE ENTERPRISE: IT, CX, AND FINANCE LEAD DEPLOYMENT

AI and analytics adoption is no longer confined to data science labs or pilot projects. The 2025 SoT survey shows that Indian enterprises are embedding these capabilities across business functions—with IT operations, customer experience (CX), and finance emerging as the most advanced areas. Meanwhile, functions like HR and marketing are still in earlier stages of experimentation and limited rollout.

The pattern reflects where the pain is sharpest—and where the payoff is clearest.

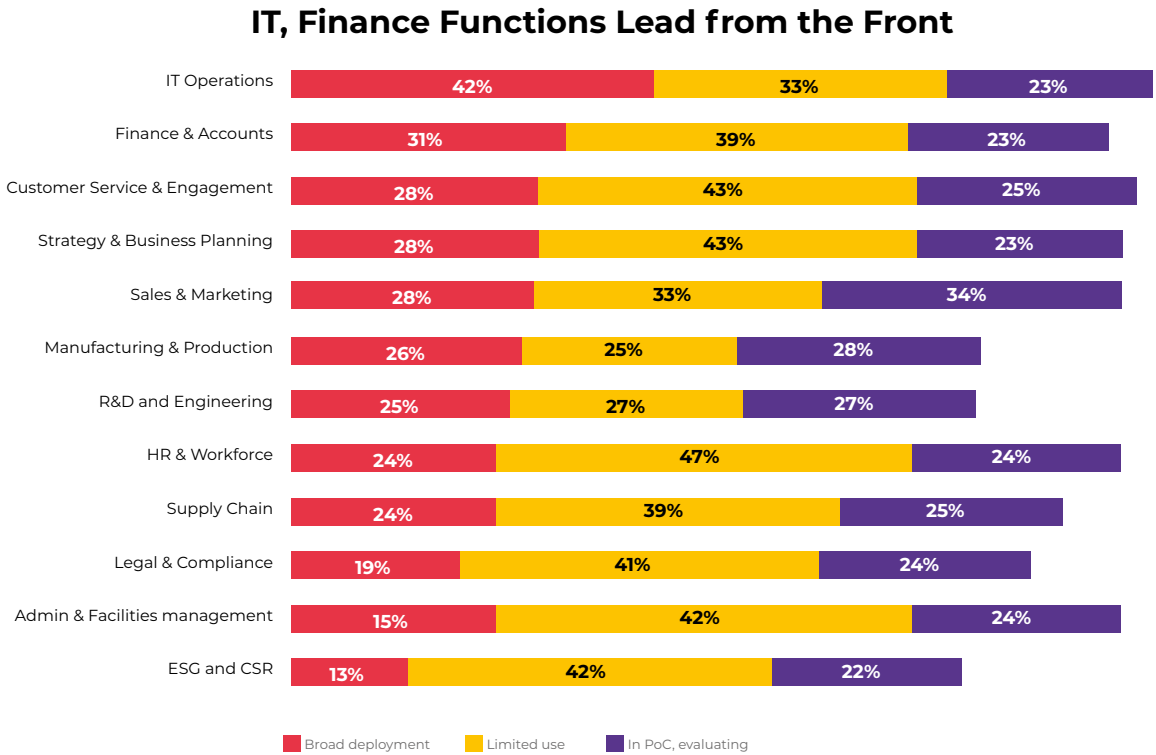

Figure 4: AI adoption is strongest in IT operations, customer engagement, and finance—lagging in HR and marketing.

Which Functions Lead in AI & Analytics Adoption?

Based on a weighted adoption score (factoring in PoCs, limited use, and broad deployment), the most AI-ready functions are:

- **IT Operations ranks highest,** with over 41% reporting broad deployment—making it the most mature AI use case in the enterprise.
- **Customer Services & Engagement** is close behind, driven by chatbots, self-service analytics,

and personalization tools.

- **Finance & Accounts and Strategy & Business Planning** show steady maturity, reflecting AI's role in forecasting, risk scoring, and scenario modeling.
- **HR & Workforce** ranks lowest among the top five—indicating slower adoption of AI in hiring, retention, or performance management processes.

Notably, all five functions show active evaluation or limited use, confirming broad interest even where deep deployment is still ramping up.

What These Patterns Suggest

- **Ops Comes First** IT operations benefit quickly from AI—via automation, anomaly detection, ticket triage, and predictive maintenance.
- **CX Drives Investment** AI is enabling faster response, better segmentation, and real-time feedback loops in customer-facing teams.
- **Finance Leads in Trust** With strong data discipline and ROI orientation, finance is a natural fit for early analytics scaling.
- **HR Is Cautious—but Curious** AI in people management raises cultural and ethical concerns—slowing adoption despite use case potential.

> IT Ops is reaping the biggest gains from AI—automating tasks, spotting issues early, triaging tickets faster, and preventing failures before they happen.

CIO Action Agenda

- Double down on AI in IT operations—not just for efficiency, but as a proving ground for enterprise-wide automation.
- Partner with CX leaders to expand AI use cases in personalization, voice analytics, and service design.
- Support finance teams with forecasting models, fraud detection tools, and spend analytics platforms.
- Work with HR and compliance to identify low-risk AI pilots—such as candidate screening, sentiment analysis, or learning personalization.

Key Insight

AI adoption reflects operational maturity and data readiness. Functions that are digitized, repeatable, and data-rich will naturally lead—those that are culture- or people-centric require more care and change management.

Takeaways for Ecosystem Partners

- **AI and analytics vendors** should provide function-specific accelerators—prebuilt models, connectors, and dashboards for ops, CX, and finance.
- **System integrators** must tailor rollout strategies based on function-specific maturity and change appetite.
- **HR tech providers** should embed explainability and governance into their AI modules to reduce adoption resistance.

Bottom Line

AI doesn't start everywhere at once—it starts where the data is clean, the value is visible, and the business is ready. CIOs must lead from the front, but support every function's journey with empathy, enablement, and alignment.

AI ADOPTION MATURITY: IT, MARKETING, AND SALES TAKE THE LEAD

AI adoption is not a binary state—it's a journey. The 2025 SoT survey shows how Indian enterprises are progressing across stages of AI maturity: from planning and piloting to limited and full deployment. IT, marketing, and sales functions emerge as the most advanced in this journey, while HR and engineering show promising momentum but lag in execution.

The front-runners are where data, automation, and measurable impact align.

IT, Engineering Lead AI Adoption, with Sales, Finance Close Behind

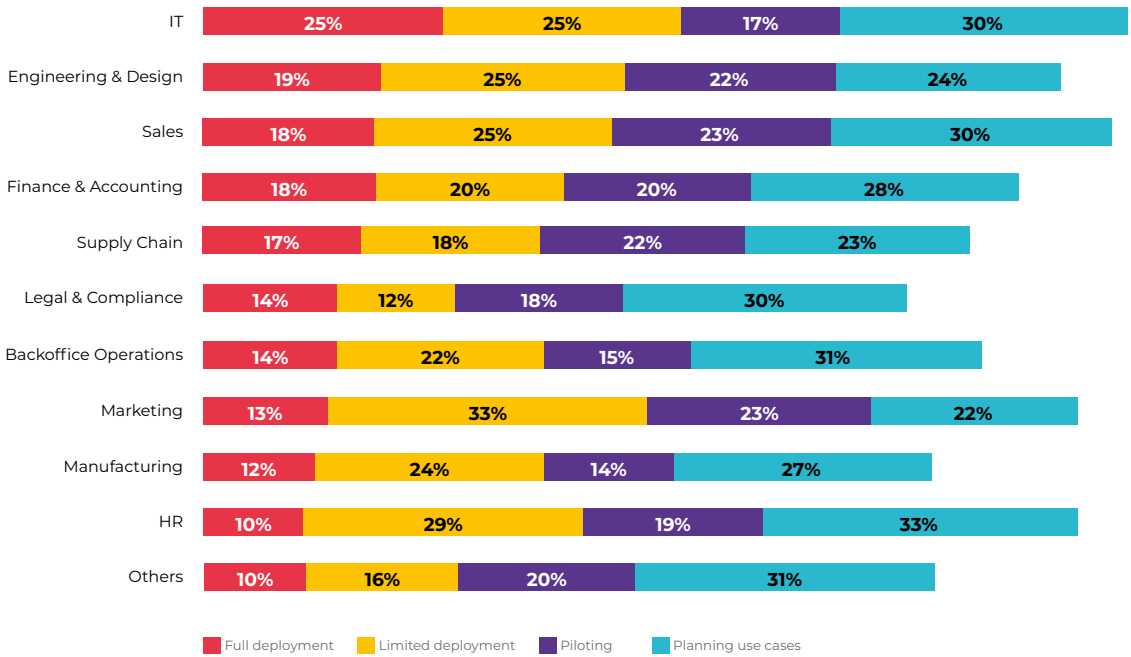

Figure 5: AI is furthest along in IT operations, marketing, and sales—HR and engineering are still gaining traction.

Which Business Units Are Most Mature in AI Adoption?

Based on a weighted scoring model (factoring in stage of adoption), the top-ranked units are:

- **IT leads with the highest maturity score (2.38)**—nearly 50% report limited or full deployment.
- **Marketing (2.22) and Sales (2.21)** follow closely, with widespread piloting and growing production use.

- **Engineering & Design (2.19)** shows mid-level maturity, likely driven by design automation and predictive simulation.
- **HR (2.00)** is in early-to-mid adoption, with a large portion still in planning or pilot phases.

These results track closely with business unit readiness, data availability, and alignment with AI-friendly use cases.

What This Tells Us About AI Traction

- **IT Is the Natural Home for AI Ops and Enablement** From ITSM to infrastructure management and SecOps, AI tools are helping automate, triage, and optimize IT workflows.
- **Marketing and Sales See Fast ROI** Personalization, lead scoring, sentiment analysis, and campaign optimization are well-defined AI use cases—with clear outcomes.
- **Engineering is Niche, but Growing** Design validation, generative prototyping, and simulation are promising, but require higher model sophistication and integration.
- **HR Faces Cultural and Ethical Complexities** While AI can assist with hiring, retention, and training, these applications need greater care in rollout and governance.

> IT tops the AI maturity curve, with marketing and sales close behind—driven by data-rich use cases and measurable impact. HR and engineering show potential but lag in execution.

CIO Action Agenda

- Treat IT as both a use case and an AI enablement layer—using internal success stories to drive broader buy-in.
- Deepen AI integrations in sales and marketing—especially in customer insights, attribution, and content generation.
- Partner with HR to identify ethical, explainable AI pilots—starting with workload prediction or training personalization.
- Help engineering teams experiment with AI-based simulation, testing, and optimization tools—with guidance from data science teams.

Key Insight

AI maturity varies by business function—and that's expected. What matters is structured progress: from idea to pilot to value. IT and customer-facing units are often the beachheads for AI scale-up.

Takeaways for Ecosystem Partners

- **AI platform vendors** should offer tailored solutions by function—pre-tuned models and analytics templates.
- **Change management consultants** can help slower-adopting units like HR navigate risk, trust, and governance concerns.
- **Integrators must** align AI solutions with functional KPIs—revenue, satisfaction, efficiency, or retention.

Bottom Line

AI maturity doesn't come all at once—it comes where readiness meets relevance. CIOs who support early movers while nurturing slower adopters will accelerate organizational AI fluency and impact.

AI AT WORK: IT OPS, CYBERSECURITY, AND CONTENT CREATION

Beyond strategy decks and pilot programs, AI is taking root in the daily mechanics of how enterprises operate. The 2025 SoT survey shows that the most intensively AI-enabled processes are those that are data-rich, repetitive, and time-sensitive—like IT monitoring, cybersecurity, and customer engagement. These are the arenas where automation, pattern detection, and rapid decisioning offer clear returns.

AI isn't changing what businesses do—it's transforming how efficiently and intelligently they do it.

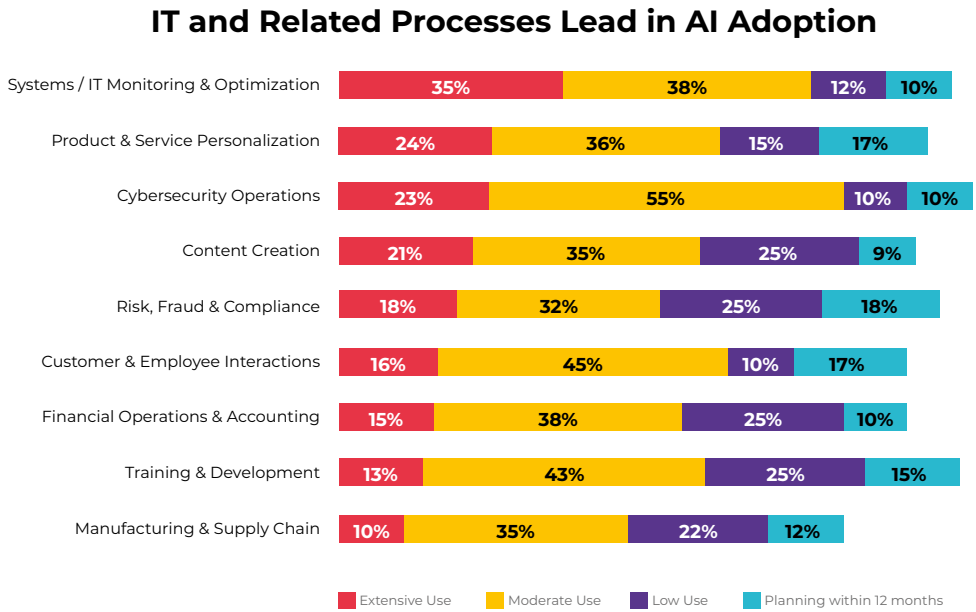

Figure 6: AI is already well embedded in monitoring, protection, and personalization processes—training and recruitment follow.

Which Business Processes Use AI the Most?

Based on an AI usage intensity score (weighted by extensive, moderate, and low use), the top-ranked processes are:

- **IT Systems Monitoring & Optimization** is the undisputed leader, with 73.3% of respondents using AI to some degree—35% extensively.
- **Cybersecurity Operations** follows closely, with over 78% already applying AI and more planning to in the next 12 months.
- **Content Creation—**driven by GenAI and NLP tools—has significant uptake, especially in marketing, communications, and CX.
- **Product & Service Personalization** also scores high, driven by recommendation engines,

behavioral analytics, and real-time targeting.
- **Training & Development** is gaining traction, with over 57% usage reported—mostly moderate or low, but growing steadily.

These patterns confirm that AI adoption is strongest where the ROI is high and the inputs are structured and voluminous.

What the Trends Reveal

- **Monitoring and Defense Are AI's First Frontier** IT and security teams benefit immediately from AI's ability to detect anomalies, triage events, and surface insights faster than manual analysis.
- **Generative Content Is Mainstreaming Fast** Enterprises are increasingly using AI to draft, adapt, and personalize content—especially at scale across customer segments.
- **CX Is a Sweet Spot** Personalization engines and real-time customer modeling are now standard features in advanced digital engagement stacks.
- **Learning Is Evolving—but Slowly** AI is entering L&D through adaptive training paths, skills mapping, and content tagging—though HR systems need time to catch up.

> About 98% participants cite cost reduction and process optimization as key drivers, proving AI is as much about streamlining as it is about scaling.

CIO Action Agenda

- Expand AI usage in monitoring and security—leveraging anomaly detection, behavioral baselining, and predictive modeling.
- Integrate GenAI into marketing workflows—balancing automation with brand integrity and editorial oversight.
- Use personalization models to enhance both CX and employee experience—across service desks, intranets, and portals.
- Partner with L&D teams to pilot AI-based training recommendations, skill gap analyses, and dynamic curriculum planning.

Key Insight

AI's strongest use cases are invisible—but indispensable. Enterprises that embed AI into core processes—not just standalone apps—will see the most sustainable gains.

Takeaways for Ecosystem Partners

- **AI vendors** should focus on embedding intelligence into existing workflows—rather than pushing standalone platforms.
- **Security and IT platform providers** must expand AI-native capabilities like self-healing infra, root-cause analysis, and intelligent alerting.
- **LMS and HR tech** players have a major opportunity to differentiate through AI-powered skills and learning analytics.

Bottom Line

AI isn't waiting for a formal roadmap—it's already in motion where it matters. CIOs must now scale these gains, monitor for risk, and bring visibility to AI's quiet, powerful role in process improvement.

ACQUIRING AI: ENTERPRISES LEAN TOWARD IN-HOUSE AI DEVELOPMENT

The decision to adopt AI is only the beginning; how it's acquired, integrated, and governed determines its long-term impact. The 2025 SoT survey reveals that Indian enterprises are showing a clear preference for building AI solutions internally—whether independently or in collaboration with partners. AI-as-a-service (AIaaS) also enjoys strong traction, while packaged solutions rank lower in preference.

Enterprises want control, flexibility, and alignment over out-of-the-box simplicity.

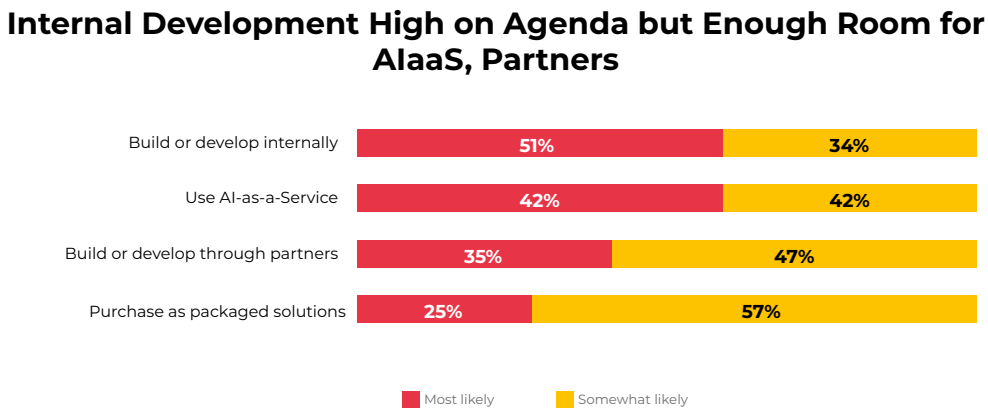

Figure 7: Internal builds and AI-as-a-service top the list of preferred acquisition modes—packaged solutions rank lower.

Preferred Modes of Acquiring AI & Analytics Capabilities

Based on combined likelihood scores (factoring "Most Likely" and "Somewhat Likely" responses), the top approaches are:

- **Build or develop internally** leads with a weighted score of 2.31—over 85% of respondents consider it a likely route.
- **AI-as-a-Service (AIaaS)** ranks next at 2.17, offering a flexible, scalable option without full ownership burdens.
- **Partner-led development** (2.08) is also popular—especially where internal expertise or resources are limited.
- **Packaged AI solutions** trail at 1.98, with only 24.6% ranking them as their most likely mode of acquisition.

This mix shows that while enterprises value speed and accessibility, they're also wary of black-box solutions that may not align with business or compliance needs.

What This Preference Mix Tells Us

- **Control and Customization Matter** Enterprises want AI that fits their specific processes, data models, and governance frameworks—not just generic functionality.
- **AIaaS Balances Agility and Access** For many, it's the right middle ground—faster than custom builds, more flexible than packaged tools.
- **Packaged Solutions Face Trust and Integration Barriers** While easier to procure, they may lack transparency, adaptability, or alignment with enterprise workflows.
- **Partners Are Enablers, Not Replacements** Collaborative development through SI partners or boutique firms is common—but with enterprises retaining architectural control.

> AI isn't plug-and-play—it's built with intent. CIOs who own the journey and embrace the right partners will unlock intelligence that drives real strategy.

CIO Action Agenda

- Invest in internal AI competencies—especially in data engineering, model governance, and DevOps for AI.
- Treat AIaaS as a tactical accelerant—but ensure integration with core IT and data platforms.
- Evaluate packaged AI tools rigorously—check for data portability, model explainability, and vendor lock-in risks.
- Use partner engagements to supplement internal builds—not substitute long-term strategy ownership.

Key Insight

Enterprises don't just want AI—they want **fit-for-purpose** AI. The dominant preference is to shape and scale AI capabilities around unique business needs and data assets.

Takeaways for Ecosystem Partners

- **Vendors and SaaS providers** must increase transparency, configurability, and integration ease in their AI offerings.
- **SI and consulting firms** should position themselves as co-builders—not just implementers—of custom or semi-custom AI stacks.
- **AIaaS providers** must offer modular APIs, strong data protections, and usage flexibility to retain enterprise trust.

Bottom Line

The AI journey is not plug-and-play—it's architected, iterated, and aligned. CIOs who own the AI development path—while remaining open to platforms and partners—will build solutions that are not only smart, but strategic.

DEPLOYMENT BARRIERS: SECURITY, DATA QUALITY, AND CHANGE MANAGEMENT TOP THE LIST

As enterprises move from AI pilots to scaled deployment, the real obstacles are less about algorithms and more about context. The 2025 SoT survey shows that concerns around data privacy, availability, and organizational change dominate the list of deployment challenges. Choosing the right tools and navigating regulatory complexity follow close behind.

AI success depends on more than just code—it depends on compliance, clarity, and culture.

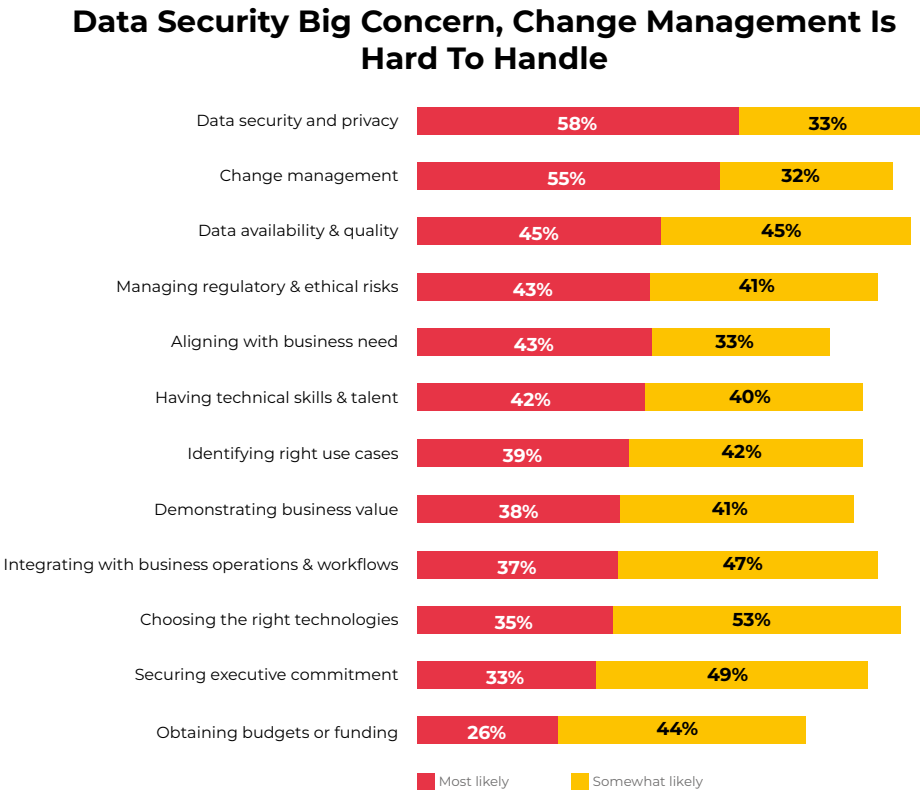

Figure 8: Enterprises cite privacy risks, data challenges, and internal resistance as key hurdles to scaling AI and analytics.

Top Challenges to Scaling AI and Analytics

Respondents rated the severity of various barriers to deploying AI and analytics. The most frequently cited challenges (by combined "High" and "Medium" concern) are:

- **Data security and privacy risks (91.7%)** top the list—confirming how central trust is to AI adoption.
- **Data availability and quality (90.0%)** remain persistent issues—especially as unstructured and siloed data grows.
- **Choosing the right technologies (88.3%)** reflects both vendor complexity and architecture tradeoffs.
- **Change management (86.7%)** is a major concern, especially as AI disrupts workflows and decision hierarchies.
- **Regulatory and ethical risks (83.6%)** show rising visibility—driven by expanding laws, audit expectations, and public scrutiny.

These results suggest that **AI's barriers are no longer mostly technical—they're strategic, operational, and human.**

What These Concerns Reveal

- **Security and Privacy Are Non-Negotiable** Enterprises know that a single misstep in data governance can derail their entire AI program—especially in regulated sectors.
- **Good Data Beats Great Models** Without reliable, complete, and accessible data, even the most advanced models fail to deliver consistent value.
- **Tool Sprawl is Real** With AI tools emerging across cloud, SaaS, and open-source ecosystems, many organizations struggle to integrate and standardize.
- **Change Fatigue and Trust Gaps Hold Back Progress** Teams often resist AI adoption if they don't understand the goals, believe in the outputs, or see how it impacts their role.

CIO Action Agenda

- Embed privacy-by-design principles in AI development—using anonymization, encryption, and consent management.
- Invest in data readiness—through cataloging, quality pipelines, and domain-specific enrichment.
- Establish a reference architecture for AI—aligning tools to governance, interoperability, and lifecycle needs.
- Prioritize change management with clear communication, hands-on enablement, and stakeholder co-design of AI use cases.

Key Insight

AI deployment isn't slowed by lack of ambition—it's slowed by uncertainty, fragmentation, and risk. Overcoming these barriers requires design thinking as much as data science.

Takeaways for Ecosystem Partners

- **Vendors** must support privacy-enhancing features, open standards, and explainable outputs.
- **Service providers** should act as translators—bridging between AI capabilities and organizational needs.
- **Change leaders and L&D partners** must prepare the workforce for AI through contextual training, coaching, and culture alignment.

Bottom Line

To scale AI, enterprises must clear the path—not just build the product. CIOs who prioritize trust, readiness, and usability will create the conditions for responsible and rapid AI growth.

CULTURE IS THE CATALYST: LITERACY, LEADERSHIP, AND LEARNING

The 2025 SoT survey confirms a powerful truth: technology alone doesn't deliver transformation—people do. For Indian enterprises advancing their AI and analytics agendas, the most critical success factors are organizational culture, leadership vision, and user enablement. Data literacy and cross-functional collaboration are seen as non-negotiables.

AI is not a bolt-on—it's a behavioral shift.

Pan-organization Data and AI Literacy, Leadership Support Are Essential for Success

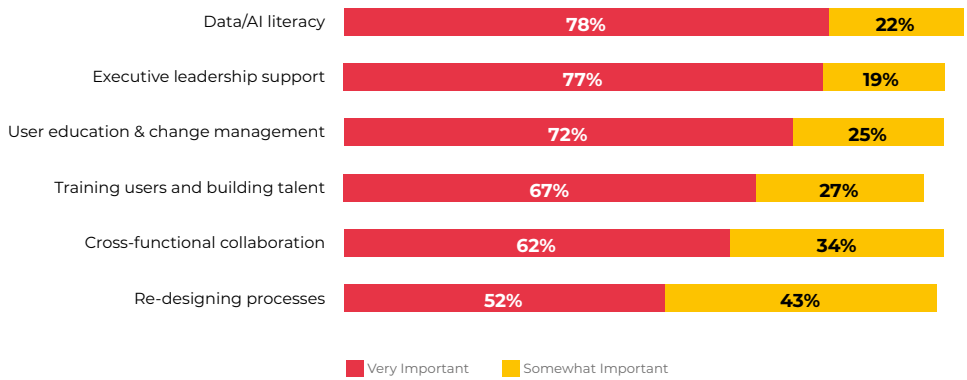

Figure 9: Enterprises say mindset and behavior matter as much as models—literacy, leadership, and collaboration top the list of enablers.

Top Cultural Enablers for AI and Analytics Success

Respondents rated the importance of various cultural factors to AI adoption and impact. The top-ranked enablers (by combined "Very Important" and "Somewhat Important" responses) are:

- **Data and AI literacy (100%)** is considered essential by every respondent—reflecting the need for foundational fluency across roles.
- **Executive leadership support (96.8%)** follows closely, confirming that top-down alignment is a powerful multiplier.
- **Cross-functional collaboration (96.7%) and user education & change management** (96.7%) are both seen as key to bridging AI's promise and day-to-day workflows.
- **Re-designing processes around AI (95.0%)** rounds out the list—underscoring that AI adoption requires rethinking, not just retrofitting.

These scores suggest that the **soft skills and structural shifts around AI matter just as much as the algorithms themselves.**

What the Culture Data Tells Us

- **Everyone Must Understand AI—Not Just Use It** Literacy is now a prerequisite for trust, adoption, and responsible usage. It demystifies the tech and empowers informed action.
- **Leadership Matters More Than Budgets** Where C-level leaders advocate for and role-model AI usage, the rest of the organization follows.
- **AI Is a Team Sport** Siloed functions struggle to realize full value. Cross-functional teams foster better problem definition, faster iteration, and broader impact.
- **Change Management Is the Long Gam** Success depends on communication, coaching, and consistency—not just rollout plans.

> Data literacy is non-negotiable—100% of respondents call it essential. Over 96% also stress the need for leadership support, collaboration, and change management to drive AI success.

CIO Action Agenda

- Launch enterprise-wide literacy programs with role-based AI training and use case storytelling.
- Ensure board and executive buy-in—not just in funding, but in ongoing sponsorship and communication.
- Embed analytics champions in business units to foster collaboration, feedback loops, and peer learning.
- Integrate change management into AI deployment plans—budgeting for adoption, not just deployment.

Key Insight

Culture determines the ceiling of AI's impact. Without trust, understanding, and collaboration, even the best tools fall short.

Takeaways for Ecosystem Partners

- **Training and L&D providers** should offer modular, context-rich literacy programs—from frontline users to executives.
- **Consultants** must address cultural readiness in every AI roadmap—through assessments, journey maps, and enablement playbooks.
- **Platform vendors** should prioritize usability, transparency, and explainability to reduce friction and build confidence.

Bottom Line

The AI journey is not plug-and-play—it's architected, iterated, and aligned. CIOs who own the AI development path—while remaining open to platforms and partners—will build solutions that are not only smart, but strategic.

AI BUDGETS SURGE: OVER 93% OF ENTERPRISES PLAN TO SPEND

If there's one signal of AI and analytics becoming core to enterprise strategy, it's the budget line. The 2025 SoT survey reveals overwhelming momentum behind AI investments in India: nearly every respondent expects spending to increase, and over half forecast a significant rise. This reflects growing confidence, maturing strategies, and intensifying competitive pressure to operationalize AI.

The experimentation phase is over—AI is now a funded mandate.

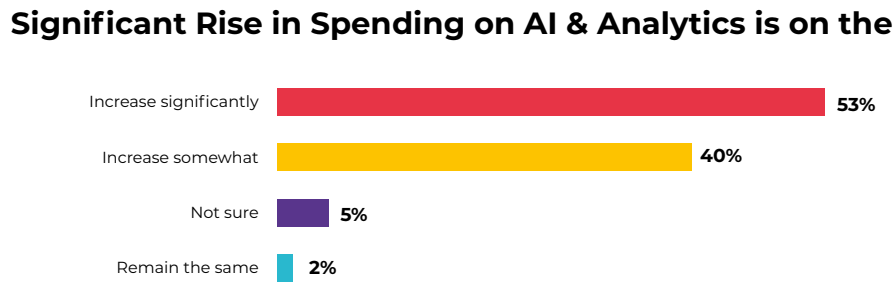

Figure 10: A resounding majority of enterprises expect to increase their AI and analytics investments—over half significantly.

Spending Outlook for AI and Analytics

Respondents were asked how their organization's spending on AI and analytics is likely to change. The results are striking:

- **53.2% expect to increase spending** significantly—indicating major transformation initiatives or scale-ups.
- **40.3% expect a moderate increase,** signaling ongoing expansion and integration of existing programs.
- **Only 1.6% expect budgets to remain the same,** and none reported plans to decrease spending.
- **4.8% remain unsure,** but are likely to follow the broader investment trajectory in the near term.

In total, **93.5% of enterprises plan to increase AI and analytics spending**—a clear inflection point for enterprise adoption.

What the Spending Patterns Reveal

- **Confidence Has Replaced Caution** Previous concerns around ROI, governance, and readiness are being overtaken by a belief that AI is essential for efficiency, innovation, and resilience.
- **AI Is Moving from Silo to System** Spending increases reflect not just new use cases, but deeper integration of AI into business systems, workflows, and decision-making.
- **Enterprises Are Investing in Scale and Skills** Budgets are expanding to fund infrastructure, talent, governance, automation, and embedded intelligence—not just pilots or proofs of concept.

Three in four CIOs expect GenAI for workload optimization to be enterprise-ready within two years—signaling strong belief in AI's operational impact beyond content generation.

CIO Action Agenda

- Anchor budget requests in cross-functional ROI—link spending to business outcomes in sales, ops, and CX.
- Balance innovation spend (new use cases) with foundational investment (data, governance, platforms).
- Establish long-term TCO models for AI infrastructure—including retraining, model updates, and change management.
- Track and communicate business impact metrics—revenue uplift, process speed, risk mitigation—to sustain executive support.

Key Insight

The AI and analytics wave is no longer driven by hype—it's driven by hard budgeting decisions. Investment signals intent, and this year's data signals enterprise-wide acceleration.

Takeaways for Ecosystem Partners

- **Vendors** should prepare for scale conversations—enterprise clients are ready to go beyond trials into strategic partnerships.
- **Consultants and integrators** must focus on operationalization, sustainability, and business alignment—not just implementation.
- **L&D providers** will see growing demand for role-specific upskilling—data fluency, AI ethics, and model management.

Bottom Line

The AI journey is not plug-and-play—it's architected, iterated, and aligned. CIOs who own the AI development path—while remaining open to platforms and partners—will build solutions that are not only smart, but strategic.

Innovation & The AI Ecosystem

Architecting Intelligence with Intent

As AI becomes enterprise-critical, Indian organizations are rethinking leadership, partnerships, and validation frameworks—transforming AI from isolated innovation into an orchestrated, accountable ecosystem.

Contents

Executive Summary

In 2025, the spotlight is on how enterprises scale AI responsibly and effectively—not just what they deploy. Indian organizations are embracing AI as a foundational enabler of business growth, but they're equally focused on governance, readiness, and ecosystem alignment.

Leadership buy-in is high: 71% say their executive leadership is fully aligned on AI adoption, and over 60% report that AI strategy ownership sits with CIOs, CDOs, or business heads. But scaling AI requires more than intent—it demands validated claims, robust vendor criteria, and innovation pathways.

Explainability (72%), scalability (71%), and integration with internal data platforms (69%) top the list of AI solution selection criteria. Simultaneously, over 84% of enterprises validate vendor claims through independent testing or cross-customer benchmarking—underscoring a cautious but confident approach to external partnerships.

Enterprises are also actively engaging with startups: 63% have worked with AI startups, yet nearly half face challenges around IP clarity, integration readiness, and long validation cycles. Co-innovation is a goal, but success requires stronger frameworks.

Internally, AI innovation is most often driven by functional business teams (48%), rather than centralized R&D—signaling a shift toward applied AI across real business processes.

The big picture: the AI ecosystem is moving from inspiration to implementation. Organizations now seek AI that is explainable, scalable, compliant, and integrative—with strong leadership at the helm and purposeful collaboration across the value chain.

AI READINESS: WHERE ENTERPRISES STAND TODAY

AI has crossed the threshold from promise to practice—but not every enterprise is moving at the same speed. For Indian CIOs, the question is no longer "Should we invest in AI?" but "How ready are we to scale it with confidence, accountability, and real outcomes?" The 2025 SoT survey reveals a market in transition. While some organizations are embedding AI into core processes and boardroom conversations, others remain stuck in isolated pilots or paralyzed by talent, cultural, or infrastructure gaps. Understanding this readiness spectrum is key to making informed decisions—both within the enterprise and across the partner ecosystem.

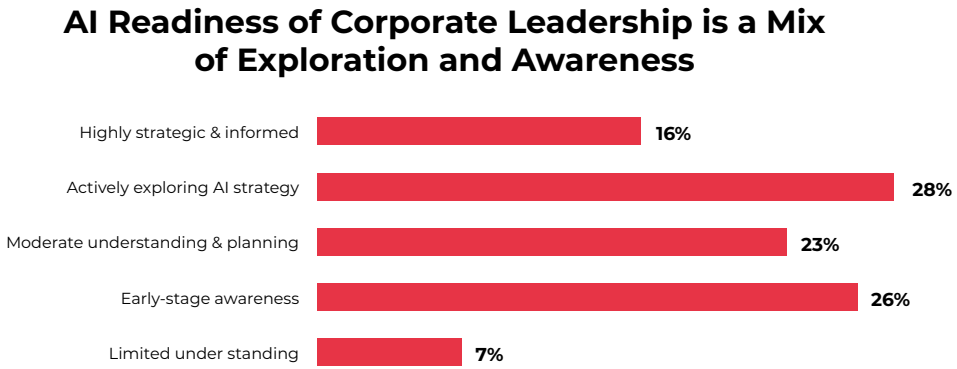

Figure 11: Over half of organizations are in early or exploratory stages of AI leadership readiness, with few truly strategic.

The Maturity Spectrum: A Market in Motion

Enterprise CIOs and tech leaders were asked to self-assess their AI readiness—from "limited understanding" to "highly strategic engagement." The responses reveal a healthy level of activity—but also significant room to grow:

- **7% report "Limited understanding"**—little to no awareness or preparedness. These firms may lack leadership sponsorship, infrastructure, or even a business case for AI.
- **26.3%** are in the **"Early-stage awareness"** phase—AI is recognized but not strategically embedded.
- **22.8%** report a **"Moderate understanding and planning"**—they're beginning to build roadmaps and talent, but execution is uneven.
- A promising **28.1%** are **"Actively exploring an AI strategy"**—often through pilots, centers of excellence, and leadership buy-in.
- Only **15.8%** are **"Highly strategic and informed"**—operationalizing AI at scale with governance, outcomes, and cultural alignment.

These findings reflect the **explosive growth of unstructured data,** compared to slower-growing structured enterprise data like logs or forms.

Key factors separate the leaders from the laggards:

- **Leadership Commitment** Strategic organizations often invest in CXO-level learning programs, dedicated AI teams, and formal governance structures. These are not just IT initiatives—they're top-down transformation agendas.
- **Data Infrastructure and Talent** Many firms in the "moderate" or "early-stage" categories struggle with fragmented data systems and a shortage of AI-literate talent. Without strong foundations, scaling remains elusive.
- **Cultural Readiness** Resistance to change, fear of automation, and lack of cross-functional collaboration often stall initiatives—even when tools and funding are available.
- **Experimentation Appetite** The most mature organizations are actively piloting, not just planning. They're willing to fail fast, learn, and iterate—often in partnership with startups or academia.

72% of enterprises rank explainability as a top AI solution selection criterion—clarity, not just capability, drives adoption.

CIO Action Agenda

- Map your current AI maturity—honestly and cross-functionally.
- Align AI pilots with strategic business goals—not just tech ambition.
- Invest in data modernization and AI literacy across functions.
- Build "scale pathways" from pilots to production—from team to enterprise.

Key Insight

While fewer than 1 in 5 enterprises are "highly strategic," **over 66% are beyond the early stage.** This signals a **huge opportunity** for acceleration—if the right levers are pulled.

Takeaways for Ecosystem Partners

- Vendors should adapt go-to-market strategies based on enterprise maturity. Early-stage firms may need advisory and change management, while strategic adopters demand co-innovation and scalability.
- Policymakers can use this segmentation to tailor skills programs, regulatory support, and funding incentives.
- CIOs must treat readiness as a journey, not a checkbox. With evolving regulations, new AI models, and changing customer expectations, agility is key.

Bottom Line

The race to AI maturity is well underway—but it's not a sprint. Enterprises that invest in foundational capabilities and cultural readiness will move from experimentation to impact faster—and with greater resilience.

LEADERSHIP ACTIONS ON AI: FROM WORKSHOPS TO WORKFORCE

Intent is no longer enough—AI now demands visible and coordinated leadership action. As AI ambitions escalate, so too does the scrutiny on how seriously enterprise leadership is preparing their organizations. The 2025 SET survey suggests that while some leadership teams are building momentum through cross-functional taskforces and formal workshops, others are lagging in critical areas like talent and advisory support.

CIOs must ask: Are we merely exploring AI, or are we building a sustained, organization-wide movement?

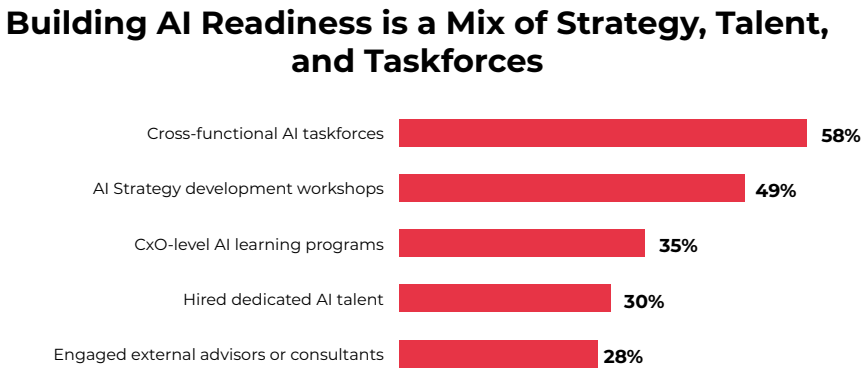

Figure 12: Cross-functional taskforces and strategy workshops lead the way, but talent gaps persist.

Where Are Enterprises Placing Their Bets?

Respondents were asked about specific measures undertaken by leadership to support AI adoption. The results show encouraging signs of cross-functional engagement—but also expose significant inconsistencies:

- **57.9% have created cross-functional AI taskforces,** indicating a clear intent to break down silos and enable enterprise-wide alignment.
- **49.1% conducted AI strategy workshops,** suggesting that structured leadership dialogue is on the rise.
- **35.1% invested in CXO-level AI learning** programs, signaling some buy-in at the top—but not yet mainstream.
- **29.8% have hired dedicated AI talent, showing progress** but underscoring the continued talent crunch.
- **Only 28.1% engaged external consultants or advisors,** which may reflect budget caution—or misplaced confidence in internal readiness.

Leadership Levers: What's Working, What's Missing

- **Cross-functional Alignment** Taskforces are helping shift AI from isolated IT projects to enterprise-wide initiatives. However, without a shared vision and accountability, these structures can become symbolic.
- **Executive Education** Learning programs for top leadership are essential—but adoption remains modest. Bridging the AI knowledge gap at the boardroom level could unlock faster decision-making and stronger governance.
- **Talent and Expertise** The limited investment in dedicated talent and external advisors may reflect internal resource constraints or overestimation of in-house capabilities.

63% have worked with AI startups, but challenges persist—IP rights, integration gaps, and long validation cycles test even the most promising collaborations.

CIO Action Agenda

- Build formal cross-functional AI leadership councils with clear mandates and timelines.
- Integrate AI themes into annual CXO offsites, leadership bootcamps, and strategic planning cycles.
- Benchmark internal capabilities—honestly—and identify where external partners can accelerate outcomes.
- Prioritize AI hiring plans that blend technical, business, and ethical fluency.

Key Insight

A majority of leadership teams are initiating cross-functional engagement and strategy sessions—but fewer are addressing talent gaps or external expertise. This imbalance could slow execution and expose enterprises to risk.

Takeaways for Ecosystem Partners

- Vendors should tailor engagements to leadership maturity. Offer workshops, readiness assessments, and structured pilot programs—not just tools and platforms.
- Policy and industry bodies can play a catalytic role by funding leadership training, supporting public-private taskforces, and incentivizing cross-sector collaboration.

Bottom Line

AI leadership is being redefined—not just by vision, but by execution. The most future-ready organizations are those that invest early in strategy, talent, and cross-functional leadership. The message is clear: AI success doesn't start in the lab—it starts in the boardroom.

WHO OWNS THE AI STRATEGY? THE RISE OF SHARED ACCOUNTABILITY

Ownership is strategy. In the AI era, the question of who owns the AI roadmap goes far beyond job titles—it's a signal of organizational readiness, ambition, and risk appetite. The 2025 SET survey reveals a landscape where AI strategy is increasingly collaborative, yet lacks a consistent anchor. While technical leaders like CTOs and CDOs are emerging as primary custodians, business leaders and CEOs are just as likely to be in the mix.

For CIOs and CXOs, the implication is clear: aligning on AI ownership is no longer optional—it's a prerequisite for effective execution.

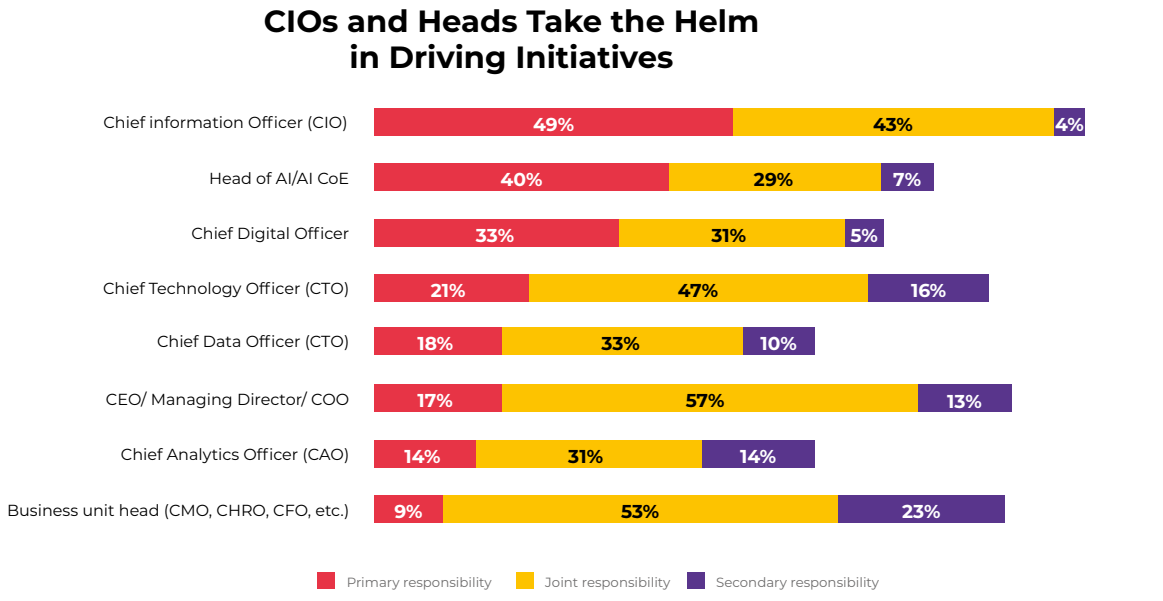

Figure 13: AI strategy ownership is fragmented—CTOs and CEOs lead, but joint responsibility is the norm.

AI Strategy: A Multi-owner Mandate

Respondents identified individuals or roles responsible for driving AI strategy. The responses reveal three major patterns:

- **Joint responsibility dominates:** Across all roles, joint ownership scores higher than primary or secondary responsibility—underscoring the collaborative (but often ambiguous) nature of AI leadership.
- **CTOs lead primary ownership:** At 20.9%, the CTO is most frequently cited as the primary AI strategy owner, followed closely by the Chief

Data Officer (17.5%) and CEO/COO (17.4%).

- **CEO-level involvement is strong: T**he CEO or Managing Director is cited as a joint owner by 56.5% of respondents—reinforcing the strategic importance of AI at the top.
- **Business unit heads rarely own AI:** Only 9.3% see BU heads as the primary owners of AI strategy, though 53.5% include them in joint leadership roles.

Ownership Matters: Why It's Not Just a Title Game

- **The Power of Joint Accountability** While collaboration is healthy, unclear ownership can stall decision-making, dilute accountability, and create competing priorities across functions.
- **The Strategic Role of the CTO** The prominence of the CTO reflects AI's deep entwinement with infrastructure and platforms—but risks becoming too tech-centric if not balanced by business ownership.
- **CXO-Level Engagement is Rising** The emergence of CEOs and COOs as visible stakeholders is a promising signal. Their involvement helps elevate AI from an operational initiative to a strategic differentiator.

> AI strategy has no single owner—CTOs, CDOs, and CEOs share the lead. As joint ownership rises, so does the need for sharper coordination and clear accountability.

CIO Action Agenda

- Establish clear governance frameworks—defining who leads, who contributes, and how success is measured.
- Ensure business and technology leaders are co-owners—not rivals—in shaping the AI agenda.
- Use AI councils or boards to institutionalize multi-stakeholder collaboration, with documented roles and outcomes.
- Map ownership across the AI lifecycle—from strategy and experimentation to implementation and ethics.

Key Insight

No single role dominates AI strategy today—but the CTO, CDO, and CEO collectively hold the reins. With joint ownership being the most cited pattern, clarity, coordination, and accountability are more critical than ever.

Takeaways for Ecosystem Partners

- Vendors must navigate multi-stakeholder buying centers—crafting engagement models that resonate across tech, data, and business functions.
- Advisors and policymakers can guide enterprises in establishing AI leadership blueprints that reflect global best practices while honoring local org structures.

Bottom Line

AI is not a solo mission. Enterprises that establish clear, cross-functional AI ownership—anchored in both tech and business leadership—will accelerate faster, manage risk better, and deliver more sustainable value. In the end, the question is not "Who owns AI?" but "Does everyone know their role in making it succeed?"

SCALING AI: WHAT'S ON THE PRIORITY LIST?

As AI transitions from innovation labs to enterprise-wide deployment, CIOs face a new mandate: scale with confidence. That means tackling the foundational, architectural, and cultural enablers that can make or break AI's impact. The 2025 SET survey reveals a clear picture of what's keeping AI leaders up at night—and what's rising to the top of their strategic agendas.

AI at scale is no longer about just choosing the right model—it's about preparing the people, processes, and infrastructure to support it.

Governance, Automation, and Business Value Are Top Priorities

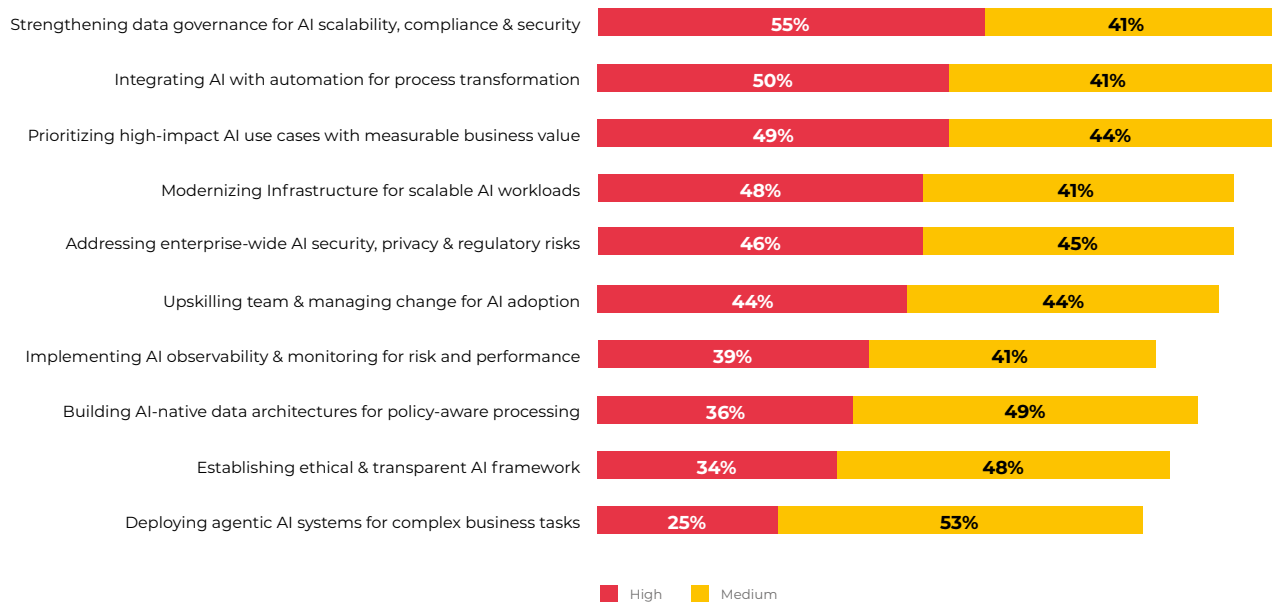

Figure 14: Talent, observability, and data readiness lead AI scale-up priorities in 2025.

Enterprise Priorities: Scaling Starts with People and Platforms

When asked to rate scaling priorities, CIOs emphasized a mix of talent development, data modernization, and operational rigor:

- **44.4% ranked "Upskilling teams and managing change" as a high priority,** the most cited response. The cultural side of AI adoption is clearly top of mind.
- **38.9% cited "AI observability and monitoring" as a top focus,** underscoring the need for

operational resilience.

- **36.4% prioritized "AI-native data architectures",** showing that legacy data systems remain a major barrier.
- **33.9% emphasized "Ethical and transparent AI frameworks",** a sign that trust-building is no longer optional.
- **Only 25.5% rated "Deploying agentic AI systems" as a high priority, reflecting caution toward m**ore autonomous use cases**.**

Notably, the "medium" priority share across most options hovers around 44–52%, indicating broad acknowledgment—but also resource constraints.

What's Driving These Priorities?

- **People before platforms** Despite the hype around new models, most CIOs are prioritizing the human infrastructure needed to make AI work—reskilling, cross-functional alignment, and change management.
- **Observability = Control** As AI enters production, CIOs are laser-focused on knowing what their systems are doing. Monitoring, drift detection, and incident response are becoming core AI capabilities.
- **Cautious on agentic AI** Enterprises are still testing the waters with autonomous or semi-autonomous AI. The perceived risk-reward ratio remains high.

> Beyond the AI hype, CIOs are investing in people—reskilling, alignment, and change management to drive real impact

CIO Action Agenda

- Develop organization-wide AI upskilling programs across roles and seniority levels.
- Invest in tools and processes for real-time AI observability and model health checks.
- Modernize data architectures with AI in mind—not just for storage, but for quality, lineage, and agility.
- Build ethics and governance frameworks into AI workflows—not as afterthoughts but as embedded design principles.

Key Insight

While automation and advanced agents grab headlines, enterprise leaders are focused on getting the basics right: people, monitoring, data, and governance. Scaling AI is a marathon—not just a model deployment sprint.

Takeaways for Ecosystem Partners

- **Vendors** must pivot from selling AI features to enabling scale—through training, monitoring tools, and ethical scaffolding.
- **Advisors** should help enterprises design AI observability architectures and guide responsible adoption of emerging agentic systems.
- **Policy influencers** can support workforce skilling programs and promote interoperable observability standards.

Bottom Line

The message is clear: the path to AI scale runs through talent, trust, and technical maturity. Enterprises that invest now in operational foundations—not just shiny tools—will turn AI into sustainable competitive advantage.

DOMAIN DEPTH OVER GENERAL CAPABILITIES PREFERRED FOR AI PLATFORMS

AI may be general-purpose in capability—but enterprises increasingly want it with a domain-specific edge. The 2025 SET survey reveals a strong preference for tailored AI solutions that speak the language of the business. Whether it's healthcare, manufacturing, BFSI, or retail, CIOs are leaning toward tools that come pre-aligned with industry use cases, regulations, and workflows.

Customization still matters—but starting with relevance seems to be the new baseline.

Figure 15: Six out of 10 CIOs prefer domain-specific AI solutions over general-purpose platforms.

What the Data Reveals

When asked to identify their organization's preferred type of AI solution or platform:

- **57.9% chose "Domain or industry-specific solutions."** These are AI platforms fine-tuned for sector-specific challenges and datasets.
- **42.1% preferred "General-purpose platforms with customizability."** These offer broad functionality but require more integration and tailoring.
- **0% indicated "No preference."** A clear sign that enterprises are thinking strategically about solution fit.

This marks a clear departure from earlier cycles, where many buyers defaulted to horizontal AI platforms due to market immaturity.

Why is Domain-Specific AI Is Gaining Ground?

- **Faster Time to Value** Sector-specific solutions reduce the need for extensive customization and shorten implementation timelines.
- **Built-In Compliance and Context** Many industries—like finance or healthcare—have unique compliance needs. Domain AI solutions often embed these constraints natively.
- **Pressure to Show Results** As scrutiny of AI investments increases, CIOs prefer solutions that can demonstrate ROI quickly—often via proven industry use cases.

58% of enterprises now prefer domain-specific solutions that deliver faster ROI, built-in compliance, and sector-ready intelligence. Strategic fit is the new priority.

CIO Action Agenda

- Evaluate industry-specific AI tools not just for functionality, but also for ecosystem maturity and roadmap alignment.
- Ensure interoperability between domain-specific solutions and enterprise data platforms.
- Use general-purpose platforms selectively—for cross-cutting use cases or in-house innovation where control is critical.
- Push vendors for transparency on training data provenance, especially in regulated industries.

Key Insight

Enterprise buyers are moving away from generic platforms and toward AI solutions that are pre-wired for their sector. This signals a maturity shift—from experimentation to execution—with results as the new north star..

Takeaways for Ecosystem Partners

- **Vendors** should double down on domain-specific capabilities, partnerships, and case studies. “Horizontal” is no longer enough.
- **Consultants and advisors** can guide enterprises in balancing domain depth with platform extensibility.
- **Policy enablers** may consider sector-focused AI sandboxes and incentives to accelerate adoption in priority industries.

Bottom Line

AI adoption is no longer about the biggest engine—it’s about the best fit. Domain-specific solutions are helping CIOs leapfrog complexity and demonstrate real outcomes faster. The future of AI is not one-size-fits-all—it’s tailor-made.

CIOS SEEK TRUST, FIT, AND FUNCTIONALITY FROM AI VENDORS

As AI adoption accelerates, the vendor landscape is expanding—and becoming harder to navigate. Enterprises are no longer impressed by AI for AI's sake. They demand solutions that work, scale, comply, and fit seamlessly into existing architectures. The 2025 SET survey uncovers a decisive shift: CIOs want practical, performant, and responsible AI—and they're scrutinizing vendors accordingly.

Choosing an AI partner today is as much about alignment as it is about innovation.

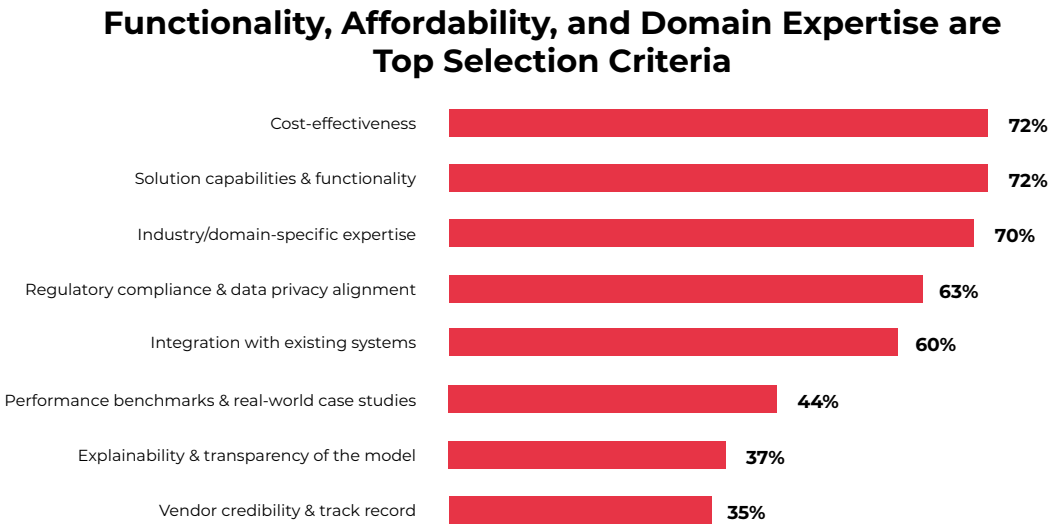

Figure 16: Solution capability and cost-effectiveness top the list, but domain expertise and compliance are rising fast.

What Matters Most in Vendor Evaluation

When asked to identify their top criteria while evaluating AI vendors:

- **71.9% cited "Solution capabilities and functionality"** as a key criterion—making it the top priority.
- **71.9% also prioritized "Cost-effectiveness",** reflecting a continued focus on ROI and budget discipline.
- **70.2% valued "Industry/domain-specific expertise",** showing the growing preference for contextual understanding.
- **63.2% emphasized "Regulatory compliance and data privacy alignment."** This is no longer a checkbox—it's a deal-breaker.
- **59.6% looked at "Integration with existing systems,"** underlining the importance of

interoperability.

- **43.9% favored vendors who shared "Performance benchmarks and case studies."**
- **36.8% emphasized "Explainability and transparency."**
- **35.1% trusted "Vendor credibility and track record."**

The findings show a blend of strategic, technical, financial, and ethical expectations—CIOs are no longer compromising on any of these.

Why This Matters: The Maturity Mandate

- **Functionality + Fit** Enterprises want AI tools that actually deliver—and plug into what they already use. Flexibility and integration are no longer fringe benefits; they're core requirements.
- **Context Over Claims** Domain knowledge and industry familiarity are now seen as competitive advantages. Vendors that can speak the customer's language stand out.
- **Governance First** Compliance, privacy, and explainability are now front-row concerns—especially in sensitive sectors like BFSI, healthcare, and public services.

> Winning vendors won't just sell AI—they'll tailor its impact to what each enterprise truly needs.

CIO Action Agenda

- Develop a standardized AI vendor scorecard across business, tech, legal, and risk dimensions.
- Prioritize pilots that demonstrate domain fit, scalability, and operational ease—not just model performance.
- Involve compliance and data governance teams early in the vendor evaluation process.
- Ask tough questions on transparency, model training data, and bias mitigation strategies.

Key Insight

CIOs today demand more than flashy demos. They want AI vendors that combine technical depth, domain expertise, cost-efficiency, and compliance readiness. In this high-stakes market, trust and traction matter more than hype.

Takeaways for Ecosystem Partners

- **Vendors** should tailor pitches to industry-specific outcomes, demonstrate integration success, and back claims with transparent benchmarks.
- **Consultants and advisors** can help enterprises create robust RFP frameworks and avoid "model washing."
- **Regulators and standards bodies** can support clearer benchmarks for explainability, interoperability, and data use policies.

Bottom Line

The AI vendor game has matured. Today's CIOs are looking for fit-for-purpose solutions—grounded in reality, rich in context, and ready for scale. The winning vendors will be those who don't just sell AI, but who understand why and how it will matter to each enterprise.

PROOF OVER PROMISE: VALIDATING VENDOR CLAIMS

In a crowded and often noisy AI vendor landscape, confidence doesn't come from claims—it comes from proof. As enterprise adoption matures, so too does the rigor with which CIOs validate vendor assertions. The 2025 SET survey reveals that enterprises are shifting from trust-based decisions to evidence-based evaluations, with pilots, internal reviews, and real-world references leading the way.

The message to vendors is clear: bring proof, not just Power Points.

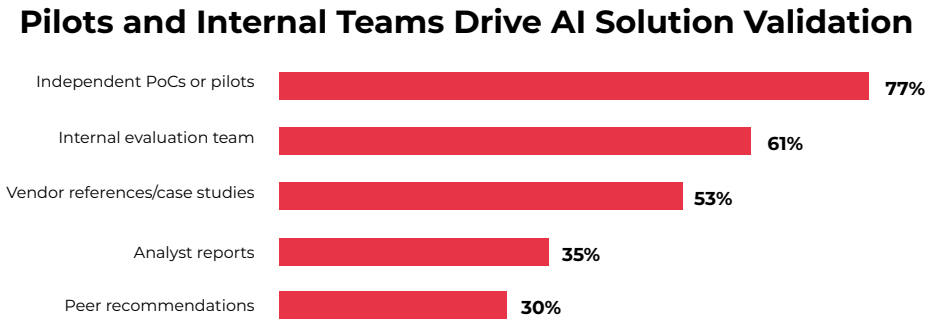

Figure 17: Independent pilots and internal evaluation teams are the top ways for CIOs to separate substance from spin.

Top Methods of Validating AI Vendor Claims

Respondents shared the methods they use to verify vendor performance, reliability, and fit. The results are unequivocal:

- **77.2% rely on "Independent PoCs or pilots"—**by far the most trusted method. Enterprises want to see AI in action before they buy.
- **61.4% use "Internal evaluation teams"** to assess vendor claims across performance, integration, and risk dimensions.
- **52.6% depend on "Vendor references and case studies"—**especially from peers in the same industry.
- **35.1% consult "Analyst reports"** for third-party validation and benchmarking.
- **29.8% lean on "Peer recommendations."**

These methods reflect a shift toward enterprise self-reliance in decision-making—powered by structured evaluation, experimentation, and peer benchmarking.

Why This Matters: The "Trust but Verify" Paradigm

- **Pilots are the New Standard** Enterprises increasingly expect vendors to demonstrate capabilities in real environments—often within weeks or months.
- **In-House Scrutiny is Rising** Internal evaluation teams ensure AI aligns with internal architecture,

compliance standards, and strategic goals—not just vendor promises.

- **Peer Proof Still Counts** References and analyst insights remain useful—but are now seen as complementary, not conclusive.

> AI buying is no longer blind trust—enterprises now demand proof, not promises.

CIO Action Agenda

- Institutionalize PoC frameworks with standardized success metrics and integration criteria.
- Equip internal teams with the tools and authority to run evaluations independently of vendor narratives.
- Maintain a vetted repository of case studies and peer feedback for ongoing vendor assessment.
- Include AI-specific validation checkpoints in the broader tech procurement lifecycle.

Key Insight

The age of vendor storytelling is over. Today's enterprise AI buyer demands proof—delivered through pilots, verified by internal experts, and reinforced with relevant case studies.

Takeaways for Ecosystem Partners

- **Vendors** must be ready to co-create PoCs, share measurable benchmarks, and engage cross-functional buyer groups early.
- **Advisors** can design repeatable validation playbooks and help enterprises scale from PoC to production.
- **Industry networks** should facilitate peer-to-peer knowledge exchange on successful vendor deployments.

Bottom Line

Buying AI is no longer a leap of faith. Enterprises are methodically stress-testing claims and demanding tangible proof of performance. Vendors that embrace transparency and co-validation will lead—not just in sales, but in long-term trust.

AI INNOVATION: CIOS VOTE FOR BIG TECH, BUT STARTUPS RISING

Innovation in AI isn't just about algorithms—it's about where they're coming from, who's commercializing them, and how fast they're scaling. The 2025 SET survey asked CIOs to identify the sources they consider most innovative in AI—and the results show a clear hierarchy, but also a few surprises.

While global tech giants still lead, homegrown startups and open-source communities are steadily climbing in relevance.

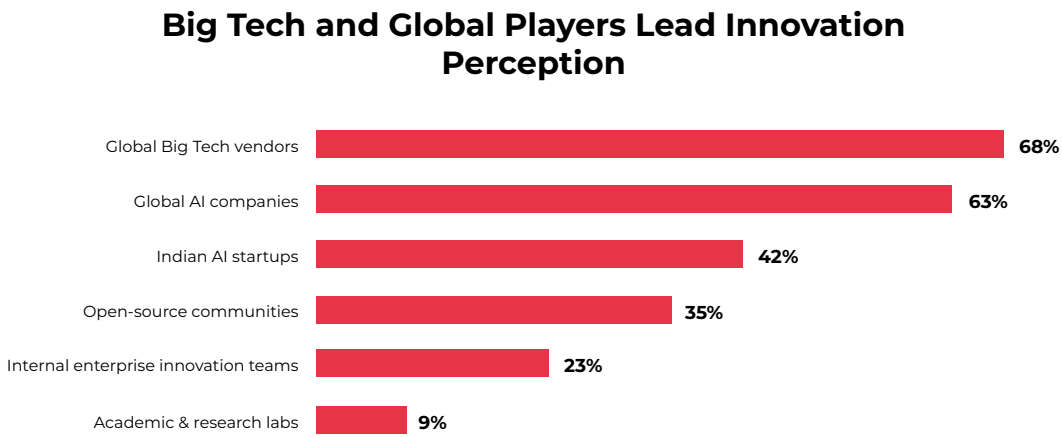

Figure 18: Global Big Tech vendors and AI specialists dominate perceptions of innovation—India's startups gain ground.

Drivers of AI Innovation

CIOs were asked where they see the most meaningful AI innovation emerging from. The responses suggest a strong belief in established players, but growing faith in emerging ones:

- **68.4% chose "Global Big Tech vendors"** (e.g., Microsoft, Google, Amazon) as top innovation sources.
- **63.2% identified "Global AI companies"** (e.g., OpenAI, Anthropic, Cohere) as key drivers.
- 42.1% cited "Indian AI startups", a notable endorsement of the local innovation ecosystem.
- **35.1% selected "Open-source communities",** pointing to the growing role of collaborative models.
- **22.8% acknowledged "Internal enterprise innovation teams."**
- **Only 8.8% credited "Academia & research labs."**

This shows that applied innovation and commercial scalability are favored over theoretical research or internal-only efforts.

Why This Innovation Map Matters

- **Big Tech Dominance Persists** With vast compute, talent, and infrastructure, global hyperscalers continue to shape AI tools and platforms used at scale.
- **Specialist AI Firms Are Influential** Companies like OpenAI and Cohere are seen as bleeding-edge, even if their enterprise models are still evolving.
- **Indian Startups are Emerging Strong** CIOs are beginning to see local firms not just as vendors—but as genuine sources of innovation tailored to Indian contexts.
- **Open-Source is on the Rise** The community-led innovation model—especially around open foundational models—is becoming impossible to ignore.

> CIOs are widening the lens—tapping startups, academia, and open-source ecosystems to co-create, pilot, and adapt AI innovations beyond traditional vendor playbooks

CIO Action Agenda

- Keep an innovation radar across startup ecosystems, open-source breakthroughs, and specialist AI firms—not just traditional vendors.
- Partner with local startups and academia for co-development, pilots, and domain-specific solutions.
- Encourage internal teams to absorb and adapt external innovations—not just invent in isolation.
- Allocate R&D budgets for ecosystem engagement, not just in-house tools.

Key Insight

While global Big Tech and specialist AI vendors still dominate the innovation narrative, CIOs are increasingly recognizing the power of local startups and collaborative ecosystems. The future of AI innovation will be distributed, not monopolized.

Takeaways for Ecosystem Partners

- **Startups** should leverage their contextual agility to build India-relevant solutions—and position themselves as co-innovators, not just suppliers.
- **Enterprises** should consider formal innovation programs that engage startups, open-source contributors, and research institutions.
- **Policy frameworks** can nurture this momentum by funding AI accelerators and public-private innovation platforms.

Bottom Line

AI innovation is no longer confined to Silicon Valley or a handful of labs. It's happening in co-working spaces, GitHub repositories, and fast-growing Indian firms. CIOs who diversify their innovation portfolio will be better prepared to build, adapt, and lead.

ENTERPRISE–STARTUP DYNAMICS: A WARMING TREND FOR COLLABORATION

AI startups are often the first to experiment, fail fast, and push the envelope. But how ready are Indian enterprises to engage with them? The 2025 SET survey suggests that startup engagement is no longer a fringe strategy—it's entering the mainstream. A combined 79.5% of CIOs say they are either "very open" or "somewhat open" to working with AI startups.

The message is clear: the doors are open—but trust, relevance, and reliability still matter.

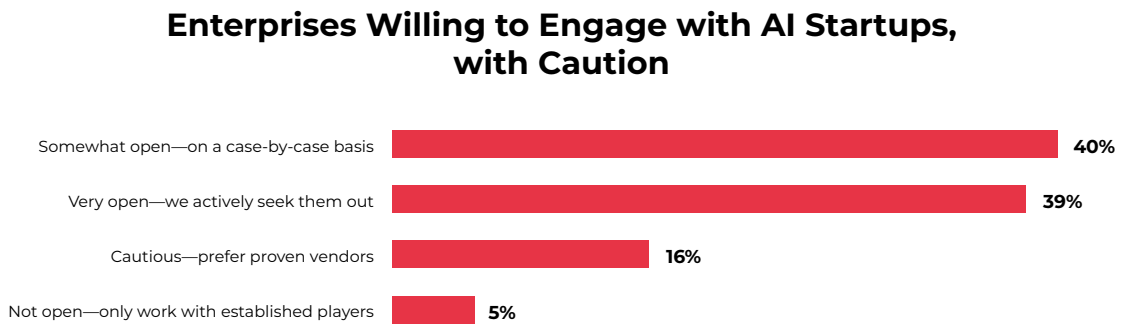

Figure 19: Nearly 80% of enterprises are open to AI startups—with a third actively seeking them out.

Where Enterprises Stand on Startup Engagement

When asked about their organization's openness to using AI solutions from startups, CIOs responded as follows:

- **640.4% said they are "Somewhat open – on a case-by-case basis."**
- **38.6% reported being "Very open – we actively seek them out."**
- **15.8% described themselves as "Cautious – prefer proven vendors."**
- **Only 5.3% are "Not open – only work with established players."**.

These results show that while enthusiasm is growing, many enterprises still want evidence of fit, scalability, and resilience before fully committing.
Scalability, and resilience before fully committing.

What's Driving the Openness—and the Hesitation

- **Startups as Innovation Engines** Enterprises increasingly see startups as key to accessing novel use cases, emerging techniques, and agile development models.
- **Risk and Resource Concerns Persist** Hesitation stems from concerns over support maturity, integration effort, and long-term viability of startups.

- **Procurement Processes Need a Refresh**
  Many enterprise procurement models are still optimized for large vendors, not nimble newcomers.

> Top performers back AI with CXO commitment, solid data infrastructure, and a culture of experimentation. It's not just IT—it's strategy.

CIO Action Agenda

- Create dedicated AI startup engagement frameworks—covering discovery, evaluation, and co-development.
- Run controlled pilots with clear success metrics to test startup offerings.
- Encourage business and IT teams to jointly evaluate startup potential—not just based on tech, but also on adaptability and partnership mindset.
- Include startups in innovation sandboxes, hackathons, and internal demo days.

Key Insight

While not without its caveats, enterprise appetite for AI startup collaboration is real—and rising. The winners will be those who combine agility with assurance, speed with scalability.

Takeaways for Ecosystem Partners

- **Startups** must articulate enterprise-relevant value and be prepared to scale proof points into production use cases.
- **Enterprises** should invest in startup onboarding mechanisms—legal, technical, and cultural.
- **Policy makers and incubators** can support curated AI startup-enterprise matching platforms and co-innovation programs.

Bottom Line

Enterprise–startup collaboration in AI is moving from "experimental" to "essential." CIOs who master the art of safe experimentation with startups will gain an edge in speed, diversity of thought, and first-mover advantage.

STARTUPS SPARK INNOVATION—BUT KEY HURDLES STILL BLOCK THE WAY

Startups bring speed, innovation, and fresh thinking. But in the world of enterprise AI, those strengths aren't always enough. The 2025 SET survey reveals the most common friction points enterprises encounter when working with AI startups—and the results highlight a fundamental truth: innovation alone can't carry a partnership. Context, compliance, and capability matter just as much.

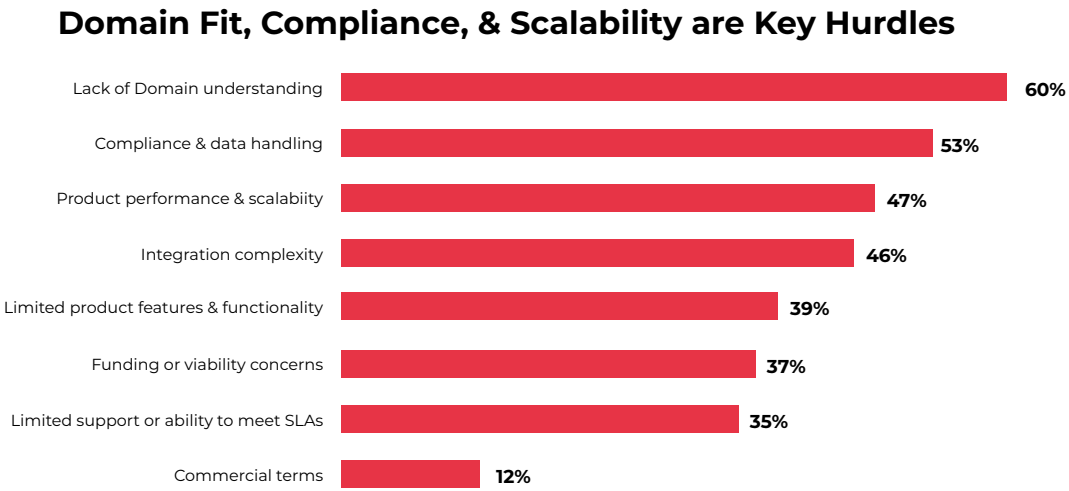

Figure 20: Lack of domain understanding and compliance readiness are the biggest barriers to enterprise–AI startup partnerships.

Top Challenges Enterprises Face When Working with AI Startups

CIOs were asked to identify the most significant challenges in engaging with AI startups. Here's what emerged:

- **59.6% cited "Lack of domain understanding."** Startups may know the tech, but often struggle to apply it within industry-specific workflows.
- **52.6% pointed to "Compliance and data handling."** This includes data residency, governance, and security protocols.
- **47.4% said "Product performance and scalability" was a concern.** Startups often excel in prototypes, but stumble in production.
- **45.6% flagged "Integration complexity"—** signaling the need for enterprise-readiness, not just clever code.
- **38.6% noted "Limited product features/ functionality."**
- **36.8% called out "Support and SLA limitations."**
- **36.8% worried about "Funding and viability risks."**
- **26.3% highlighted "Risk perception among internal stakeholders."**

- **12.3% reported issues with "Commercial terms."**

These responses show a convergence of strategic, operational, and reputational risks that must be managed for startups to succeed in enterprise environments.

Why These Hurdles Matter

- **Enterprise AI is Complex** Even innovative solutions fail if they don't speak the enterprise's language—both literally (in data formats) and metaphorically (in compliance, performance, and integration).
- **Trust and Maturity Are Key** CIOs need confidence that a startup can not only deliver value—but stay the course through scale and support.

> AI startups offer innovation, but a lack of domain fit, compliance, and scalability limits impact. CIOs seek partners, not just prototypes.

CIO Action Agenda

- Develop readiness rubrics for evaluating AI startups on domain understanding, architecture fit, and compliance posture.
- Co-innovate through controlled pilots with mutual learning cycles.
- Insist on documentation, security protocols, and support commitments—even in early stages.
- Advocate for internal champions to mitigate resistance and build shared accountability.

Key Insight

The enterprise–AI startup relationship thrives on innovation—but survives on reliability, relevance, and readiness. Bridging this gap is key to unlocking mutual value.

Takeaways for Ecosystem Partners

- **Startups** must mature quickly—by investing in compliance, support, and integration layers without compromising agility.
- **Enterprises** should create "safe zones" to experiment with startups while safeguarding risk.
- **Incubators, VCs, and accelerators** should groom startups for enterprise fit—not just funding rounds.

Bottom Line

AI startups are indispensable innovation partners—but they need to evolve from builders to business enablers. CIOs who help shape that evolution—through tough love, clear metrics, and committed pilots—will accelerate enterprise impact while helping shape the next wave of India's AI champions.

Application Development

Fast, Intelligent, and Built for Change

App modernization is no longer about catch-up—it's about keeping up. Enterprises are redesigning their application environments for agility, intelligence, and end-to-end integration.

Contents

Executive Summary

In 2025, Indian enterprises are aggressively modernizing their application estates to align with digital-era imperatives: speed, intelligence, interoperability, and user-centricity. The shift is visible across strategy, tooling, and execution.

A clear majority (76%) cite refactoring legacy apps as a top modernization priority. This is closely tied to the adoption of microservices, DevOps, and container-based architectures, which have become central to how modern apps are built and deployed.

Cloud-native applications are gaining momentum, with 51% of enterprises reporting that over half of their apps are now built for cloud environments. App development maturity is rising as well—61% say they follow structured DevOps and CI/CD practices, while only 6% remain in an ad-hoc development stage.

AI is being actively embedded into apps and workflows. Top use cases include personalization, prediction, and intelligent automation. Meanwhile, low-code/no-code (LCNC) platforms are gaining legitimacy—over 78% are already using or planning to use LCNC tools for internal and customer-facing applications.

Key challenges remain: technical debt (68%), integration across systems (67%), and limited talent availability (66%). Yet enterprises are responding with robust strategies—embracing API-first designs, modular development, and platform thinking to reduce complexity and increase scalability.

Application KPIs have matured too. Success is now measured by business agility, time-to-market, and developer productivity, not just stability or cost.

In 2025, applications are no longer static assets—they are adaptive engines of innovation, continuously evolving with business needs and technological shifts.

MODERNIZATION GATHERS MOMENTUM: AUTOMATION AND APIS LEAD THE CHARGE

App modernization is no longer an IT aspiration—it's an enterprise imperative. As organizations respond to evolving user expectations, agility demands, and digital service delivery pressures, their modernization playbooks are maturing. The 2025 SoT survey reveals a shift from lift-and-shift approaches to more strategic, architecture- and automation-led transformation.

CIOs are being asked not just to update apps—but to future-proof them.

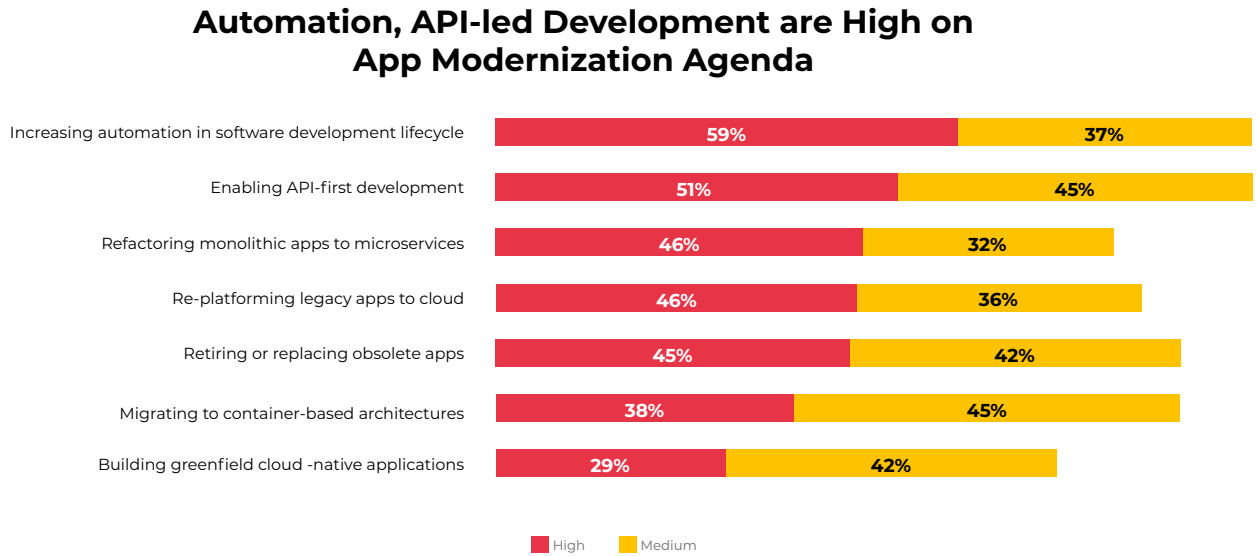

Figure 21: Enterprises prioritize automation, APIs, and re-architecture as key levers for modernization.

What CIOs Are Prioritizing Now?

When asked about their top app modernization priorities, CIOs outlined a sharp pivot toward structural upgrades and developer efficiency:

- **58.6% selected "Increasing automation in software development and operations"** as their highest priority. The focus is on speed, scale, and stability.
- **50.7% rated "Enabling API-first development" highly,** reflecting a desire for modularity, reusability, and integration readiness.
- **46.4% said "Refactoring monolithic apps to microservices"—**underscoring a shift to more granular, scalable architectures.
- **45.7% chose "Re-platforming legacy apps to cloud",** signaling continued migration momentum.
- **44.9% prioritized "Retiring or replacing obsolete apps."** Cleanup is as important as modernization..

Meanwhile, “building greenfield cloud-native apps” and “migrating to container-based architectures” are notable—but sit slightly lower on the priority ladder.

Interpreting the Shift: From Platform Shift to Productivity Focus

- **Automation as a Strategic Lever** Beyond CI/CD, organizations are automating testing, release cycles, monitoring, and incident response—pushing toward DevOps and AIOps maturity.
- **API-First Isn’t Optional Anymore** Whether for internal agility or ecosystem integration, APIs are now central to both design and deployment.
- **Microservices vs. Monoliths** The appetite to decompose legacy systems is strong—but enterprises are treading carefully, often balancing re-architecture with stability.

> 76% of enterprises say refactoring legacy apps is a top priority—modernization is no longer optional, it’s a foundational mandate.

CIO Action Agenda

- Audit existing application portfolios against modernization potential, strategic value, and technical debt.
- Invest in automation toolchains that cut across development, QA, deployment, and ops.
- Drive API enablement as a shared mandate—across product, engineering, and integration teams.
- Prioritize modernization efforts that align with user impact, agility goals, and cost control.

Key Insight

Modernization is no longer synonymous with “cloud migration.” Enterprises are looking to reshape how apps are built, integrated, and maintained—with automation and APIs at the heart of the transformation.

Takeaways for Ecosystem Partners

- **Vendors** must help enterprises go beyond “re-platforming” to rethinking app lifecycle workflows—especially around DevOps, observability, and API governance.
- **Consulting and services providers** can support decision frameworks around what to rehost, replatform, refactor, or retire.
- **Policy makers and skilling bodies** should support DevOps, microservices, and cloud-native skill development at scale.

Bottom Line

Indian enterprises are past the tipping point on app modernization. The next wave is about purposeful architecture choices and intelligent automation—not just lifting old apps into new environments. CIOs who combine deep tech fluency with cross-functional alignment will modernize faster—and smarter.

CLOUD-NATIVE ADOPTION: WIDESPREAD AWARENESS, UNEVEN PENETRATION

Cloud-native architecture has become synonymous with agility, scalability, and modernization. Yet, despite years of advocacy and adoption efforts, most Indian enterprises are still only partway through the cloud-native transformation. The 2025 SoT survey exposes a reality check: while the direction is clear, the journey remains gradual and uneven.

The question is no longer if cloud-native is strategic—but how far organizations have progressed in operationalizing it.

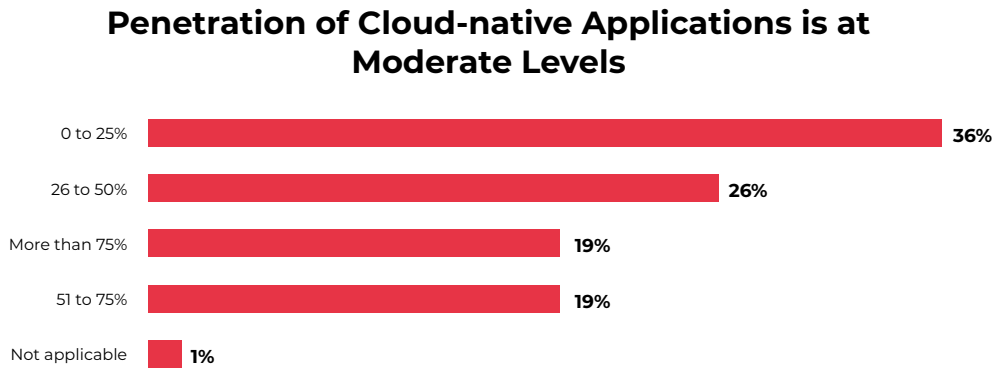

Figure 22: Over 60% of enterprises report less than half of their apps are cloud-native—only 18.6% cross the 75% mark.

How Cloud-native Apps Stack Up Today

When asked what share of their enterprise application portfolio is currently cloud-native, CIOs responded:

- **35.7% reported cloud-native penetration at 0–25%—**still early in the journey.
- **25.7% are in the 26–50% range,** marking steady but partial adoption.
- **18.6% said 51–75% of their apps are cloud-native.**
- **18.6% claimed over 75% penetration,** indicating strong cloud-native maturity.
- **Only 1.4% reported "Not applicable."**

This distribution indicates a bell-curve-shaped maturity curve, with most enterprises falling in the early-to-mid adoption zone.

Decoding the Pace of Adoption

- **Hybrid Reality Prevails** Most enterprises are juggling a mix of monoliths, replatformed apps, and truly cloud-native builds.
- **Cloud-native ≠ Cloud-hosted** Many organizations conflate cloud deployment with cloud-native design—this data suggests the

architectural transition is far from complete.

- **Skill, Tooling, and Culture Are Key Barriers** Moving to cloud-native isn't just a technology shift—it demands new mindsets around automation, DevSecOps, and composability.

> Over 78% are using or planning LCNC tools—speed, scale, and user empowerment are reshaping the enterprise app development toolkit.

CIO Action Agenda

- Assess cloud-native adoption not just by app count, but by architectural fitness, modularity, and readiness for change.
- Invest in refactoring skills and DevOps maturity to extend cloud-native benefits across more of the portfolio.
- Build standardized blueprints for cloud-native application development across business units.
- Partner with hyperscalers and SIs who can accelerate re-architecture journeys—not just migration.

Key Insight

The cloud-native wave is well underway—but most enterprises are still riding in the shallow waters. Only one in five has crossed the 75% mark, revealing a major opportunity for acceleration through architectural modernization and automation.

Takeaways for Ecosystem Partners

- **Cloud providers and SaaS vendors** must support not just cloud adoption—but architectural modernization journeys.
- **Service providers** should differentiate on cloud-native refactoring capabilities—not just lift-and-shift.
- **Policy and skilling initiatives** can support open-source cloud-native tools, developer upskilling, and DevOps training at scale. Policy makers and skilling bodies should support DevOps, microservices, and cloud-native skill development at scale.

Bottom Line

Cloud-native is a catalyst—not a checkbox. Enterprises that push beyond partial adoption and embrace modular, scalable app architectures will be better positioned for agility, resilience, and AI-readiness.

MATURITY OF ENTERPRISE APP DEVELOPMENT PRACTICES

Application development has become the engine room of enterprise digital strategy. Yet, not all organizations are equally equipped when it comes to execution discipline, architecture fluency, and innovation agility. The 2025 SoT survey shines a light on how Indian enterprises assess their app development maturity across five strategic practices.

The takeaway? Foundational engineering practices are solidifying—while frontier technologies like AI are still in early phases of adoption.

DevOps Practices Quite Mature, Other Areas at Varying Stages.

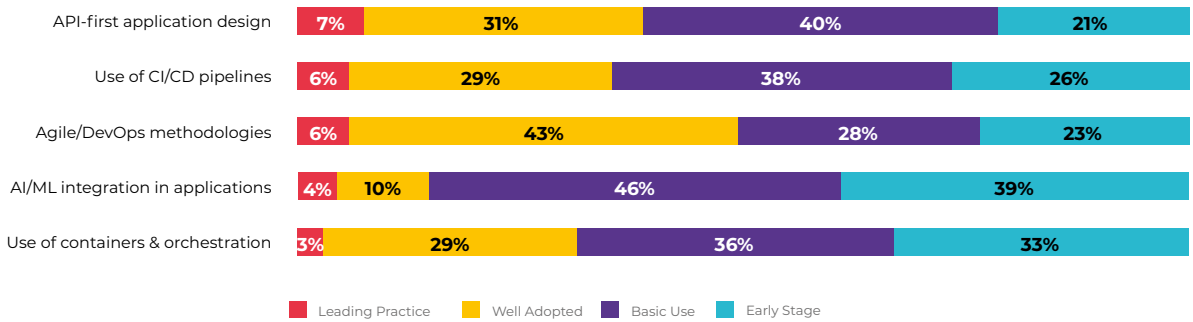

Figure 23: Agile, APIs, and CI/CD are maturing—but AI integration still lags in most organizations.

What Enterprises Are Doing Well—and Where They're Catching Up

Respondents rated their maturity across five critical app dev capabilities. The combined percentage of "Well Adopted" and "Leading Practice" responses reveals clear strengths and gaps:

- **49.3% say Agile/DevOps methodologies are well adopted or a leading practice.**
- **38.6% report maturity in API-first application design,** showing strong architectural momentum.
- **35.3% indicate solid adoption of CI/CD pipelines.**
- **31.4% feel confident in using containers and orchestration—**though still evolving.
- **Only 14.5% report maturity in integrating AI/ML into applications,** signaling a long runway ahead.

Conversely, AI/ML and even containers show significant shares in the "Early Stage" category, suggesting slow maturity curves.

Decoding the Patterns

- **Agile is Becoming Institutionalized** Nearly half the enterprises have moved beyond pilot to scaled Agile and DevOps practices—especially in

regulated and digitally native sectors.

- **API-first is Gaining Traction** As microservices and modularity become norms, API design thinking is moving upstream.
- **CI/CD and Containerization Need Reinforcement** Many enterprises still struggle with consistent pipelines, governance, and automation at scale.
- **AI Integration Still Experimental** While interest is high, actual embedding of AI/ML into applications remains fragmented—often limited to PoCs or isolated features.

> Enterprises are strong on Agile and APIs, but still catching up on AI/ML integration and container adoption, revealing uneven maturity across app dev capabilities.

CIO Action Agenda

- Invest in cross-functional DevOps enablement, with KPIs tied to deployment velocity and stability.
- Promote API-first design principles across product, architecture, and engineering teams.
- Prioritize maturity in CI/CD pipelines to support continuous delivery—not just automation for its own sake.
- Build AI-readiness frameworks that guide how, where, and when to embed intelligence into apps.

Key Insight

While foundational practices like Agile and APIs are maturing, most enterprises are still climbing the ladder on automation, orchestration, and AI integration. The gap between ambition and execution is narrowing—but only for those who invest consistently in tooling, talent, and culture.

Takeaways for Ecosystem Partners

- **Vendors** should align offerings with different maturity levels—from DevOps bootstrapping to API lifecycle governance and AI app services.
- **Advisors and coaches** can play a vital role in scaling Agile, refining CI/CD, and helping product teams think AI-natively.
- **Upskilling initiatives** must bridge not just dev talent gaps, but also architecture and ML fluency.

Bottom Line

Enterprise app development is no longer about speed alone—it's about structured speed, sustainable innovation, and intelligent design. CIOs who raise maturity across the stack will unlock compounding returns in agility, resilience, and user experience.

CONNECTING THE DOTS: APP INTEGRATION GETS AN OVERHAUL

As applications multiply and digital workflows sprawl across systems, integration has become a make-or-break capability. The 2025 SoT survey shows that while enterprises are moving away from legacy patterns like point-to-point integration and ESBs, there's still a long road ahead to achieve unified, API-first, and cloud-native integration architectures.

Integration isn't just about connectivity—it's about velocity, visibility, and control.

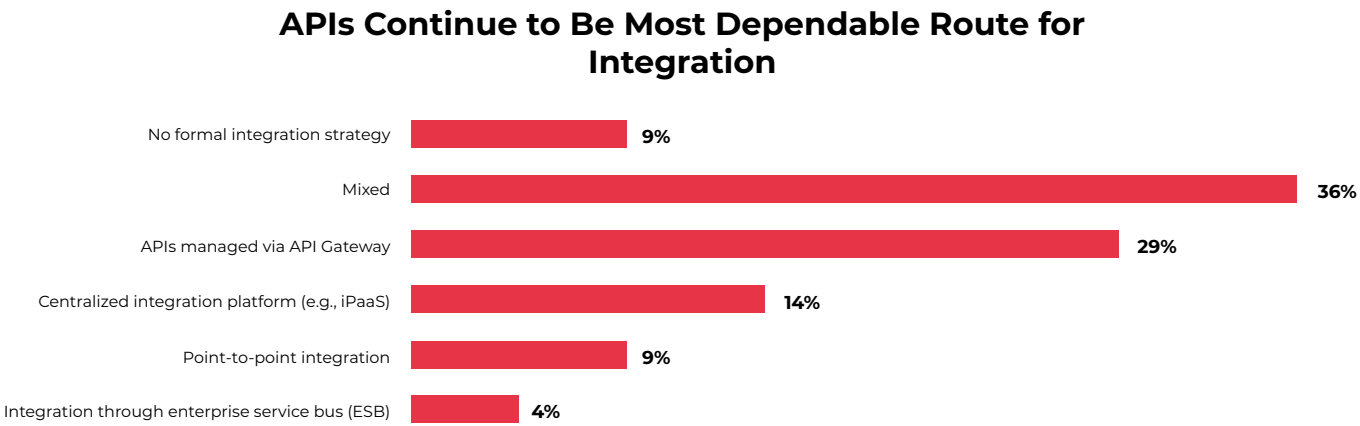

Figure 24: A third of enterprises follow a mixed integration model—API Gateways gaining ground on legacy approaches.

Current Enterprise Integration Approaches

When asked how they currently approach application integration, CIOs revealed a landscape in transition:

- **35.7% follow a "Mixed" approach—**blending legacy tools, APIs, iPaaS, and ad HOC methods.
- **28.6% use "APIs managed via API Gateway,"** pointing to growing maturity and governance.
- **14.3% rely on a "Centralized integration platform (e.g., iPaaS)."**
- **8.6% still use "Point-to-point integration."**
- **8.6% admitted having "No formal integration strategy."**
- **4.3% continue to use "Enterprise Service Bus (ESB)" solutions.**

The data reflects both the evolution underway and the fragmentation that still persists across integration layers.

Why Integration Still Lags Behind Modernization

- **Legacy Ties Run Deep** Many core systems still require ESB or custom-built connectors, slowing down transition to APIs or event-driven models.
- **API Governance Isn't Fully Mature** While

adoption of API gateways is encouraging, full API lifecycle management—versioning, security, monitoring—remains a challenge.

- **iPaaS Isn't Yet Mainstream** While cloud-native integration platforms offer powerful capabilities, adoption is slower due to perceived complexity or cost.
- **Mixed Models Reflect Reality** The hybrid nature of enterprise environments often forces CIOs to mix and match tools—highlighting the need for convergence, not just coexistence.

> CIOs must map weak links, adopt robust API platforms, treat integration as a product, and prioritize iPaaS solutions that scale with ease.

CIO Action Agenda

- Map current integration architectures and identify areas of duplication, fragility, or latency.
- Invest in API management platforms that support observability, access control, and developer self-service.
- Treat integration as a product—with roadmaps, user stakeholders, and SLAs.
- Evaluate iPaaS options not just for technical features but for ease of onboarding and cross-system extensibility.

Key Insight

A majority of enterprises still operate in hybrid integration environments—with APIs gaining traction, but legacy and manual methods still in play. Streamlining integration is critical to unlocking agility, scalability, and security in the app ecosystem.

Takeaways for Ecosystem Partners

- **Vendors** must support enterprises in bridging from hybrid to unified integration stacks—while ensuring performance and cost efficiency.
- **Advisors c**an help design scalable integration architectures and rationalize tool choices.
- **Developers and architects** need ongoing skills in API management, event-driven systems, and iPaaS workflows.

Bottom Line

Integration strategy is the silent backbone of digital transformation. CIOs who elevate integration from a back-end concern to a front-line enabler will accelerate delivery, reduce technical debt, and scale AI and automation more effectively.

WHAT'S HOLDING BACK APP MODERNIZATION?

The case for app modernization is well established—but translating intent into execution remains complex. The 2025 SoT survey reveals the stubborn challenges CIOs face in turning legacy systems into agile, scalable platforms. From skill shortages to technical debt, these barriers are slowing down transformation despite high organizational urgency.

The modernization roadmap is often less about choosing the right tools—and more about overcoming the right constraints.

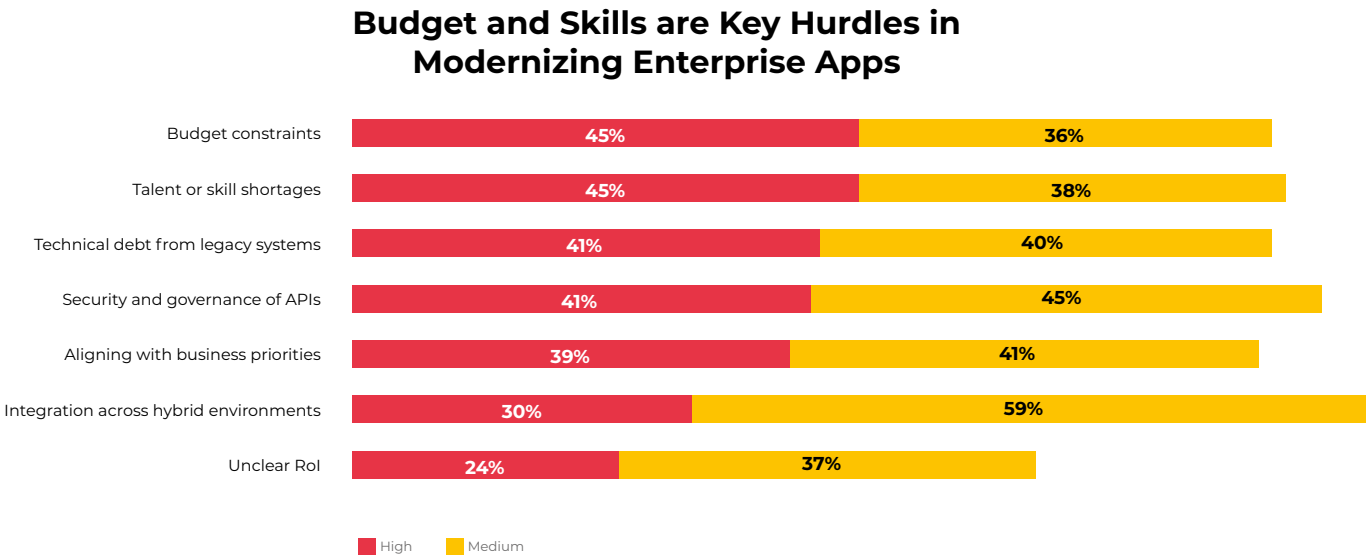

Figure 25: Talent gaps, budget pressures, and legacy debt emerge as the biggest barriers to progress.

Top Enterprise Challenges in App Modernization

CIOs rated their biggest obstacles across technical, organizational, and financial domains. The percentage of respondents citing each as a "High" challenge reveals the pressure points:

- **44.9% face "Talent or skill shortages,"** underscoring the growing demand for DevOps, cloud-native, and full-stack expertise.
- **44.9% also report "Budget constraints" as a major hurdle,** especially amid competing transformation priorities.
- **41.4% are constrained by "Technical debt from legacy systems."**
- **40.6% cite "Security and governance of APIs" as a pressing concern.**
- **38.6% struggle with "Aligning with business priorities."**

Across the board, "Medium" challenge levels were also high—showing that many of these issues are persistent, if not yet acute.

What These Challenges Reveal

- **Skills Are the Top Bottleneck** Modernization requires not just tools—but talent fluent in containers, microservices, CI/CD, API design, and architecture modernization.
- **Funding Strains Persist** App modernization often competes with newer digital investments like AI or customer experience—and may lack clear ROI metrics.
- **Legacy Baggage Is Heavy** Old tech stacks, undocumented code, and brittle systems make transformation expensive and risky.
- **API Risk is Underestimated** As APIs proliferate, governance, versioning, and security are emerging as weak spots.
- **Business-IT Alignment Still Needs Work** Without shared KPIs or clear value narratives, modernization efforts risk being deprioritized or misunderstood.

> App modernization isn't just about tech, it's about talent gaps, tight budgets, and legacy baggage holding teams back!

CIO Action Agenda

- Build a modernization business case around agility, cost reduction, and risk mitigation—not just tech debt.
- Invest in targeted skilling programs—internal and external—to reduce dependency on niche experts.
- Develop API governance policies that balance openness with control.
- Use modernization as a bridge to align IT capabilities with business strategy—via shared roadmaps and ROI scorecards.

Key Insight

Modernization is less about technology readiness and more about organizational capacity—skills, funding, governance, and strategic clarity. Enterprises must tackle these root issues to accelerate outcomes.

Takeaways for Ecosystem Partners

- **Vendors** and SIs must support capability-building alongside delivery—through tooling, templates, and embedded coaching.
- **Advisors** can help with technical debt assessments, prioritization frameworks, and modernization roadmaps.
- **Policy makers and skilling bodies** can play a catalytic role by bridging the application engineering talent gap.

Bottom Line

The modernization journey is real—but rarely smooth. CIOs who confront talent, alignment, and architecture challenges head-on will clear the runway for innovation, resilience, and growth.

APP DEV STRATEGY: HYBRID RULES, MODERN METHODS STILL EMERGING

Agility is the aspiration—but legacy rhythms still shape how many enterprises build and ship software. The 2025 SoT survey confirms what many CIOs experience daily: application development and deployment is a patchwork of old and new. While a few have made the leap to cloud-native, microservices-first architectures, most organizations are navigating a transitional phase—where hybrid models dominate.

Figure 26: Over half of enterprises follow a hybrid strategy combining Agile/DevOps with traditional methods.

Where Are Enterprises on App Dev Strategy?

When asked to describe their prevailing approach to application development and deployment:

- **55.7% said they follow a "Hybrid"** model—combining Agile/DevOps for new apps and traditional methods for legacy systems.
- **14.3% still operate with "Traditional" models,** such as waterfall and staged releases.
- **Only 10% have adopted a "DevOps-oriented" approach with CI/CD automation.**
- **Another 10% have gone "Full Agile, cloud-native, microservices-first."**
- **10% mostly rely on "external vendors/partners."**

The picture that emerges is one of pragmatic evolution—not wholesale disruption.

What the Hybrid Reality Tells Us

- **Transformation Is Uneven** Most enterprises have pockets of maturity—DevOps squads or cloud-native initiatives—but struggle to scale practices across the app estate.
- **Legacy Still Shapes the Delivery Rhythm** Apps tied to core systems often remain on traditional SDLCs, delaying modernization and slowing overall velocity.
- **Outsourcing Is Still Common** Many organizations rely on partners for specialized

app builds, maintenance, or modernization—especially in talent-constrained areas.

- **Modern Practices Are Gaining Ground—Slowly** While adoption of full-stack, cloud-native development is real, it's far from universal.

> Today's application strategy is about coexistence, not convergence. Smart CIOs aren't chasing uniformity—they're mastering the hybrid zone to drive scale, speed, and resilience across a multi-speed enterprise.

CIO Action Agenda

- Segment the app portfolio by delivery maturity—and tailor governance and tooling accordingly.
- Define a target state for application delivery (e.g., DevSecOps-first) and build transitional roadmaps.
- Create centralized enablement squads that guide Agile and CI/CD adoption across business units.
- Where partners are involved, enforce engineering standards aligned with internal practices.

Key Insight

The dominant app delivery model in Indian enterprises is hybrid—where Agile ambitions coexist with waterfall realities. To evolve, CIOs must manage both transformation and integration—modernizing the whole without breaking the parts.

Takeaways for Ecosystem Partners

- **Vendors** and integrators must align with hybrid delivery models—offering flexibility, compatibility, and gradual modernization pathways**.**
- **DevOps consultants and trainers** can focus on upskilling blended teams and bridging Agile-traditional divides.
- **Tooling providers** should support interoperability across CI/CD, ITSM, and observability platforms.

Bottom Line

Application strategy today is defined by coexistence, not convergence. The smartest CIOs aren't chasing purity—they're orchestrating progress across a multi-speed, multi-model environment. Those who manage the hybrid zone effectively will be better prepared for scale, speed, and stability.

AI IN THE APPLICATION STACK: FROM ASSISTANTS TO AUTOMATION

The next wave of enterprise value from AI lies not in standalone tools—but in AI that is embedded into applications, workflows, and user experiences. The 2025 SoT survey shows promising early adoption, especially in conversational interfaces and developer productivity tools. However, deeper integration into business-critical systems and real-time user journeys remains a work in progress.

The shift is on—from using AI to building with AI.

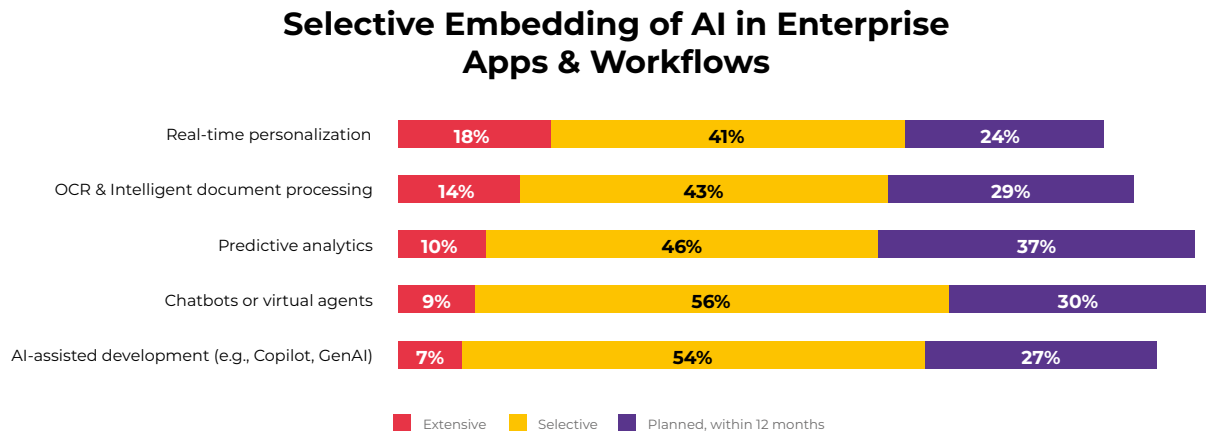

Figure 27: AI is gaining traction in chatbots and developer tools—predictive and personalized apps are catching up.

Where AI is Being Embedded Today

CIOs were asked to indicate the extent of AI integration across various use cases. Active usage (extensive + selective) paints the clearest picture:

- **64.3% report embedding "Chatbots or virtual agents."**
- **61.4% use "AI-assisted development tools"** (e.g., GitHub Copilot, GenAI code assistants).
- **58.8% deploy "Real-time personalization"** in apps or interfaces.
- **57.2% use "OCR and intelligent document processing."**
- **55.7% rely on "Predictive analytics"** to guide operations or decisions.

Planned adoption (within 12 months) is also high—especially for predictive and personalized experiences—showing a clear intent to deepen AI integration.

Reading the Trendlines

- **Chatbots Are the Entry Point** As customer expectations evolve, chat and voice interfaces are becoming standard in both B2C and B2B interactions.
- **Developer Tools Are Gaining Rapid Traction** GenAI assistants are boosting productivity—especially in writing, reviewing, and debugging code.

- **Deeper Intelligence Still Emerging** Real-time AI use cases like personalization and predictive analytics are growing—but need better data and orchestration.
- **Enterprise-Grade AI Needs Maturity** Integration into business-critical processes (e.g., finance, operations, HR workflows) is still limited due to trust, explainability, and system readiness.

> AI integration today is pragmatic and purpose-driven. CIOs are embedding it where it matters most—chatbots, code assistants, personalization, and predictive insights—balancing quick wins with long-term scale.

CIO Action Agenda

- Map AI embedding opportunities across customer experience, developer enablement, and back-office automation.
- Prioritize use cases with a clear business owner, data maturity, and repeatable workflows.
- Standardize API access, model integration, and security across AI-infused services.
- Partner with product and design teams to align AI experiences with user expectations and governance norms.

Key Insight

AI is becoming part of the app fabric—not just an add-on. But real business impact will come from consistent, context-aware, and well-governed integration—not isolated experiments.

Takeaways for Ecosystem Partners

- **AI platform vendors** must support modular, API-driven integration and offer building blocks for embedded AI.
- **Dev tool providers** can accelerate AI assistant adoption via plugins, secure model access, and code-aware contexts.
- **Policy and compliance leaders** should guide safe embedding of AI in regulated and customer-facing apps.

Bottom Line

AI's promise lies not just in capability—but in placement. Enterprises that learn to embed AI where it matters—contextually, securely, and visibly—will define the next generation of intelligent experiences.

WHAT DOES SUCCESS LOOK LIKE?

Application modernization isn't just a technical project—it's a strategic investment. But how do enterprises know it's paying off? The 2025 SoT survey reveals the key metrics CIOs use to evaluate success—and highlights a growing shift toward performance, user experience, and business alignment over just engineering efficiency.

In the race to modernize, what gets measured ultimately drives what gets improved.

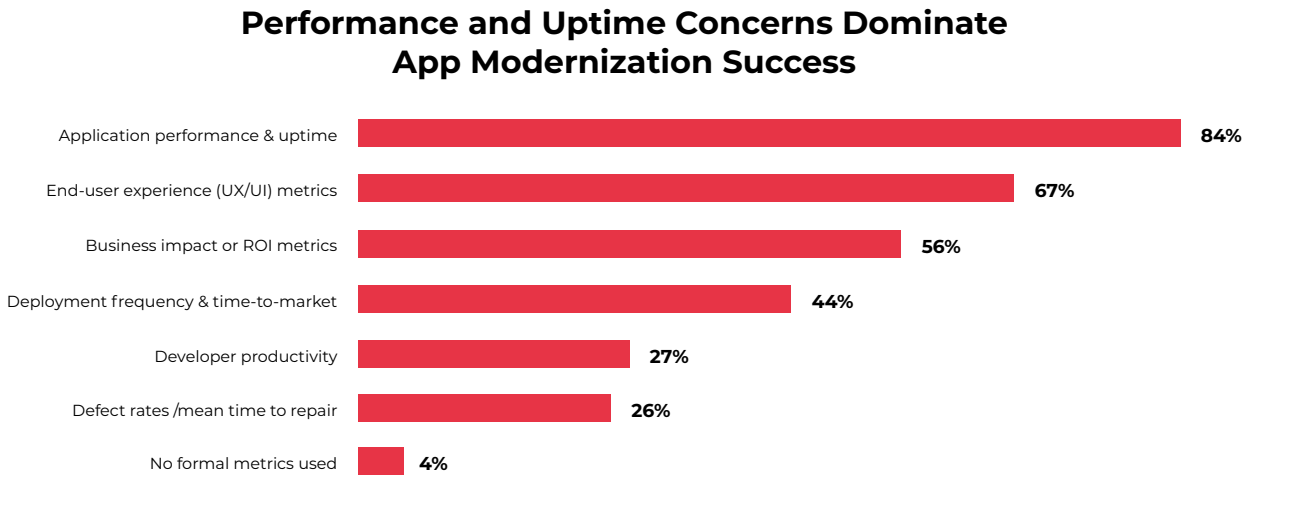

Figure 28: Performance and UX/UI top the KPI list—developer productivity trails as a formal metric.

The Most Used KPIs for App Modernization

CIOs identified the metrics they actively use to track modernization outcomes. Here's what stood out:

- **84.3% track "Application performance and uptime"—**the single most common success metric.
- **67.1% rely on "End-user experience (UX/UI) metrics,"** reflecting a strong focus on usability and engagement.
- **55.7% monitor "Business impact or ROI metrics,"** suggesting a growing maturity in linking tech work to business goals.
- **44.3% use "Deployment frequency and time-to-market" metrics—**a core DevOps indicator.
- **Only 27.1% measure "Developer productivity."**
- **4.3% reported having "No formal metrics"** to evaluate modernization success.

This distribution reflects a balance of operational, experiential, and strategic outcomes—though gaps remain in internal efficiency measurement.

Why These Metrics Matter

- **Performance = Trust** In both internal and external-facing systems, reliability and speed are table stakes.
- **UX as a Proxy for Value** As more apps go digital-first, experience design becomes a leading indicator of business adoption.
- **Business Impact Still Evolving** While more than half of CIOs use ROI-linked metrics, there's opportunity to deepen financial accountability and transparency.
- **Developer Efficiency Needs Focus** The low emphasis on developer productivity is surprising, especially given its impact on velocity and morale.

> Modernization without measurement is momentum without direction. CIOs must link app evolution to impact—tracking UX, DevOps metrics, and ROI to ensure progress is visible, valuable, and business-aligned.

CIO Action Agenda

- Align KPIs with modernization goals—whether they target agility, stability, cost savings, or user satisfaction.
- Establish consistent frameworks for collecting and analyzing UX and performance data.
- Collaborate with business units to define and track ROI metrics that link tech to outcomes.
- Integrate developer productivity metrics (e.g., cycle time, DORA metrics) into modernization dashboards.

Key Insight

Modernization success is increasingly being judged by end-user impact and performance—not just completion of replatforming tasks. But without internal metrics around engineering velocity and value creation, enterprises may struggle to sustain progress.

Takeaways for Ecosystem Partners

- **Platform vendors** must provide built-in observability and analytics to support real-time performance and UX tracking.
- **Consultants** can help enterprises define KPI trees and ROI baselines tailored to app modernization.
- **Tooling providers** should support developer experience monitoring to surface bottlenecks and drive productivity improvements.

Bottom Line

In app modernization, success isn't about transformation for its own sake—it's about outcomes. Enterprises that define, track, and evolve the right KPIs will drive greater alignment, investment confidence, and long-term impact.

APIS: FROM CONNECTORS TO CATALYSTS IN THE APP ECONOMY

APIs are no longer just technical enablers—they're strategic assets. The 2025 SoT survey affirms that Indian enterprises are steadily deepening their use of APIs for integration, interoperability, and partner enablement. However, advanced use cases like monetization and platform ecosystem expansion are still early-stage.

The role of APIs is evolving—from internal bridges to business accelerators.

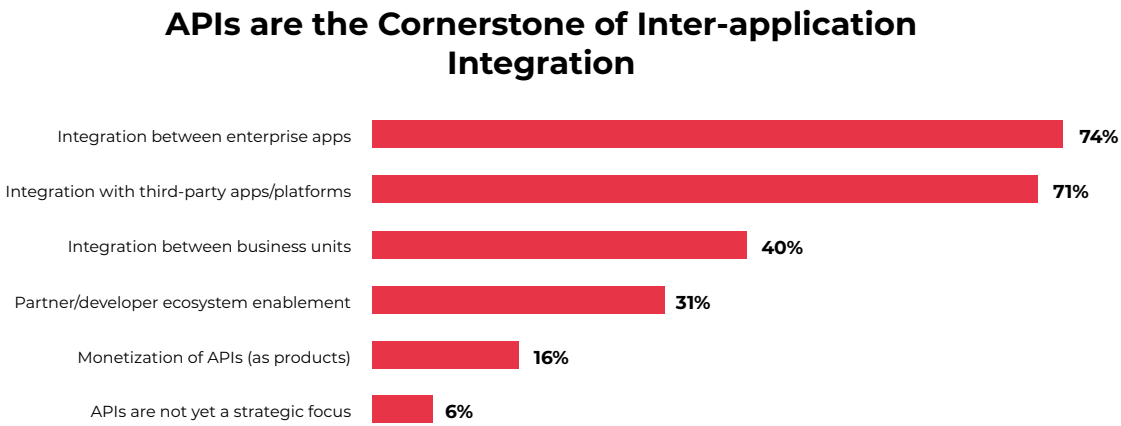

Figure 29: Internal and third-party integration lead API usage—monetization and ecosystem plays still maturing.

Where APIs Are Making the Most Impact

CIOs shared how APIs are currently being used within their application strategy:

- **74.3% use APIs for "Integration between enterprise apps."**
- **71.4% enable "Integration with third-party apps/platforms."**
- **40% facilitate "Integration between business units" using APIs.**
- **31.4% use APIs for "Partner/developer ecosystem enablement."**
- **15.7% are exploring "Monetization of APIs" as products.**
- **Only 5.7% say APIs are "Not yet a strategic focus."**

This clearly shows that integration remains the primary driver of API strategy today.

What These Patterns Reveal

- **APIs = Integration Backbone** APIs are core to internal interoperability—particularly in hybrid and multi-cloud environments.
- **Third-Party Connectivity is a Close Second** SaaS adoption and ecosystem partnerships are fueling the need for external API exchanges.

- **Internal Federation Gaining Traction** As businesses become more modular, APIs are helping unify data and processes across functions.
- **Platform Thinking Still Nascent** While some digital natives are monetizing APIs, most traditional enterprises have yet to build productized API strategies.

> With formal governance, prioritized reuse, and business-aligned KPIs, APIs are powering agility, ecosystem play, and new revenue models.

CIO Action Agenda

- Formalize API governance across lifecycle—design, security, versioning, analytics.
- Prioritize high-impact APIs for internal reuse and external exposure through developer portals.
- Align API metrics with business outcomes—not just technical calls.
- Explore monetization opportunities with APIs that deliver unique data, workflows, or services.

Key Insight

APIs are already central to enterprise integration—but their next wave of value will come from treating them as products, not just pipes.

Takeaways for Ecosystem Partners

- **API platform** vendors should support not just gateway and security, but also developer experience, monetization, and analytics.
- **Consulting partners** can help enterprises define API taxonomies and federated governance models.
- **Startups and digital platforms** should integrate with enterprise APIs to foster co-innovation and embedded partnerships.

Bottom Line

APIs are now non-negotiable in application strategy. The leaders of tomorrow will be those who go beyond connectivity—and harness APIs to accelerate agility, grow ecosystems, and create new revenue streams.

LOW-CODE NO-CODE: GAINING INTEREST, YET TO ACHIEVE SCALE

Low-code and no-code (LCNC) platforms promised a revolution in application development—faster delivery, broader participation, and reduced dependence on full-stack developers. But the 2025 SoT survey reveals a more nuanced reality: while interest is high and experimentation is underway, widespread deployment remains limited.

LCNC is not being dismissed—but it's far from being fully embraced.

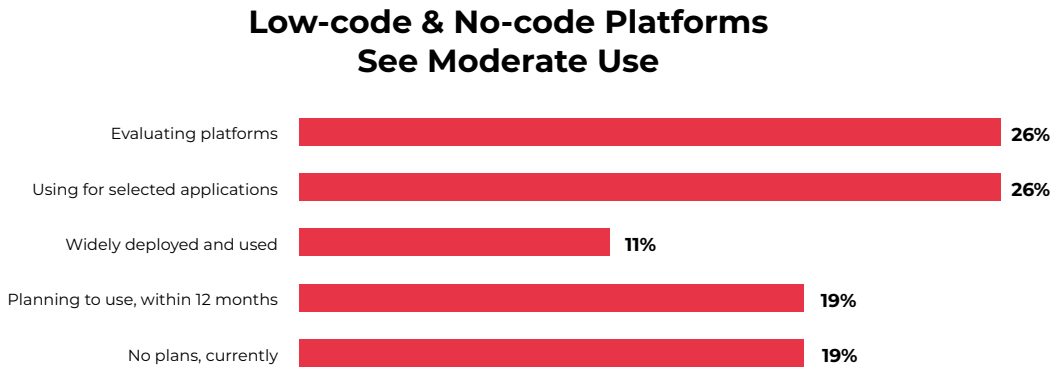

Figure 30: Most enterprises are evaluating or selectively adopting low-code platforms—broad deployment still rare.

Where Enterprises Stand on Low-code Strategy

CIOs described their organization's current LCNC posture. The data reflects a market still in transition:

- **25.7% are "Using LCNC for selected applications"—**most often for internal workflows, forms, or dashboards.
- **25.7% are "Evaluating platforms,"** reflecting growing curiosity but cautious rollout.
- **18.6% currently have "No plans."**
- **18.6% are "Planning to use within 12 months."**
- **Only 11.4% say LCNC is "Widely deployed and used."**

This distribution highlights a middle-heavy adoption curve—with a few leaders, some skeptics, and a large segment actively exploring.

Decoding the Hesitation

- **Use Cases Still Narrow** Most enterprises deploy LCNC tools for specific, low-risk applications—rarely for customer-facing or mission-critical systems.
- **Governance Concerns Persist** Shadow IT, version control, security, and platform lock-in remain top concerns for CIOs.
- **Developer Skepticism** Many engineering teams are wary of platform constraints and long-term maintainability.

- **Skills and Change Management Gaps**
  Business users need training, and IT needs clear governance to enable “citizen development” safely.

> While not yet core to enterprise app strategy, CIOs are embracing LCNC for targeted efficiencies—accelerating delivery in specific use cases without compromising governance

CIO Action Agenda

- Identify well-scoped, low-risk use cases—like internal portals, approval workflows, or quick prototypes.
- Establish guardrails for LCNC usage: access control, approval workflows, data governance, and platform standards.
- Pilot LCNC in partnership with business users—co-develop success metrics and iterate based on feedback.
- Evaluate platform roadmaps for integration capabilities, scalability, and exit strategies.

Key Insight

Low-code/no-code is no longer fringe—but it isn’t fully mainstream either. Enterprises are cautiously optimistic, using LCNC for targeted efficiencies—not yet as a core dev strategy.

Takeaways for Ecosystem Partners

- **LCNC vendors** must prove enterprise-grade security, governance, and extensibility—not just ease of use.
- **Service providers** can help enterprises design LCNC frameworks, build reusable components, and train internal users.
- **IT and business leaders** must collaborate on LCNC operating models—balancing speed with control.

Bottom Line

Low-code isn’t a silver bullet—but it can be a smart complement. Enterprises that treat it as a strategic capability—governed, integrated, and business-aligned—will unlock faster outcomes without compromising on control or coherence.

Cloud & Infrastructure

Scaling with Purpose, Building for AI

Cloud is no longer just an infrastructure decision—it's a strategic enabler for AI, agility, and modernization. Indian enterprises are aligning cloud with performance, innovation, and trust.

Contents

Executive Summary

The cloud journey in India has matured. In 2025, SaaS is firmly entrenched, with 70% of enterprises using it in production. IaaS (68%) and aPaaS (58%) are close behind, while Security-as-a-Service (SECaaS) is gaining traction, especially in regulated sectors.

Cloud hosting decisions have become more application-aware. Public cloud dominates for office productivity and collaboration, while private and hybrid clouds are favored for ERP, SCM, backup, and DR—reflecting a thoughtful balance between performance and control. Meanwhile, AI workloads are pushing infrastructure to evolve, with 64% of enterprises stating their current setups are ready—or being upgraded—for AI/ML support.

The top drivers for continued cloud investment remain: digital innovation (87%), infra modernization (68%), and faster provisioning (63%). However, cloud is now expected to deliver business outcomes, not just uptime.

Security remains top-of-mind. 80% of enterprises rate cloud security concerns as "very important," especially around configuration control, data exposure, and multicloud management. Enterprises are adopting unified visibility platforms, cloud-native IAM, and rethinking their posture for zero-trust environments.

Looking ahead, enterprises are doubling down on AI-in-cloud innovations. Over 66% expect AI to enhance orchestration and reduce costs, while many look forward to ethics-aware, domain-specific AI capabilities in cloud services over the next 12–18 months.

In 2025, the cloud is no longer the destination—it's the foundation. The intelligent enterprise builds not just on scalable infrastructure, but on purposeful, AI-ready, and secure cloud ecosystems.

CLOUD SERVICES: SAAS MATURES, EMERGING MODELS STILL EVALUATED

Cloud adoption is now mainstream—but not all services are created equal. While Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS) are firmly entrenched in enterprise production environments, more specialized offerings like Platform-as-a-Service (PaaS), Desktop-as-a-Service (DaaS), and Security-as-a-Service (SECaaS) still have a long way to go. The 2025 SoT survey reveals a clear hierarchy of adoption and intent—useful for CIOs benchmarking cloud maturity and planning future investments.

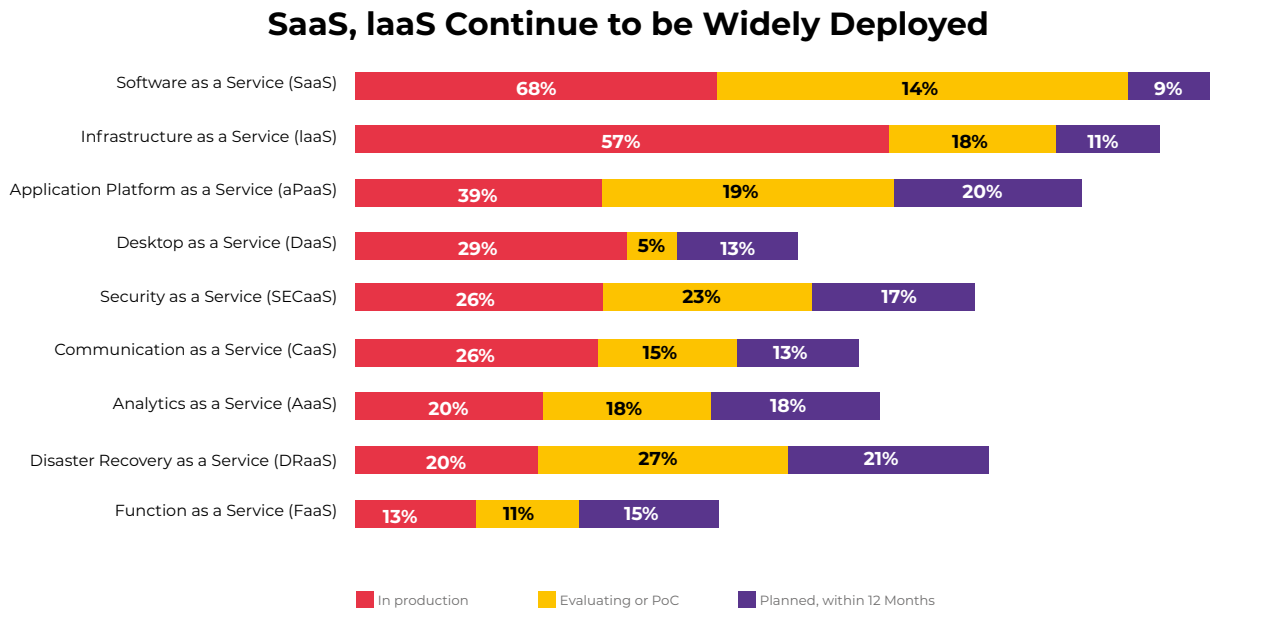

Figure 31: SaaS and IaaS dominate cloud production use—FaaS, SECaaS, and DaaS remain exploratory.

What Services Are in Production—And What's Next?

Respondents were asked to indicate the current status of various cloud service types. Here's where the adoption curves stand:

- **68.4% have SaaS in production,** making it the most mature cloud model by far.
- **57.1% have deployed IaaS,** solidifying its role as a foundation layer.
- **38.9% are using aPaaS (Application PaaS) in production,** with another 20.4% planning adoption.
- **29.1% use DaaS (Desktop-as-a-Service),** though over half (52.7%) have no plans for it.

- **26.4% run SECaaS (Security-as-a-Service),** with both high evaluation and planning interest..

Additionally, services like **Analytics-as-a-Service, DRaaS, and FaaS show** strong evaluation/planning momentum, indicating the next wave of cloud adoption.

Interpreting the Trends

- **SaaS is Ubiquitous** From productivity suites to CRM and HRMS, SaaS adoption is mature, well-integrated, and often business-led.
- **IaaS is Strategic Infrastructure** Enterprises are using IaaS as the elastic backbone for hosting apps, data, and hybrid workloads.
- **PaaS Adoption is Gaining Ground** PaaS is increasingly seen as critical for modern app development—but success hinges on DevOps and integration maturity.
- **SECaaS and DaaS Still Face Barriers** Security concerns, customization needs, and endpoint variability may be slowing broader adoption of these services.

> 87% of enterprises say digital innovation is the top driver for cloud adoption—modern infrastructure is now inseparable from business strategy.

CIO Action Agenda

- Review cloud service portfolio by strategic impact, usage depth, and architectural alignment.
- Accelerate PaaS and SECaaS adoption through internal capability building and platform partnerships.
- Explore targeted adoption of DaaS where remote work, standardization, or compliance create pressure.
- Use pilot programs and PoCs to assess newer cloud service models—especially FaaS and AaaS.

Key Insight

Enterprises have moved decisively on SaaS and IaaS—but are still experimenting or cautiously expanding into platform, function, and security services. A full-spectrum cloud strategy requires deeper engagement beyond just compute and licenses..

Takeaways for Ecosystem Partners

- **Vendors** must tailor engagement based on service maturity—advisory for early-stage services, scalability for entrenched ones.
- **Service providers** can help enterprises operationalize newer models like aPaaS, DRaaS, or FaaS by providing playbooks and migration support.
- **Policymakers** and industry bodies should promote cloud-native design, standardization, and security-readiness through skilling programs and interoperability frameworks.

Bottom Line

Cloud maturity is layered. The next frontier lies not in expanding infrastructure but in unlocking differentiated value from platforms, automation, and embedded security. CIOs who manage this layered transformation will build cloud strategies that scale with the business—not just with compute needs.

APPLICATION HOSTING: PRODUCTIVITY AND WEB LEAD CLOUD SHIFT, INDUSTRY APPS STILL HYBRID

Despite years of cloud-first narratives, application hosting across Indian enterprises remains deeply hybrid. The 2025 SoT survey shows that while office productivity tools and customer-facing web services have migrated substantially to the public cloud, core enterprise systems and vertical applications still span a mix of on-prem, private cloud, and transitional architectures.

CIOs today are orchestrating across environments—not abandoning one for another

On-prem Leads in Application Hosting, Some Wins for Private and Public Clouds

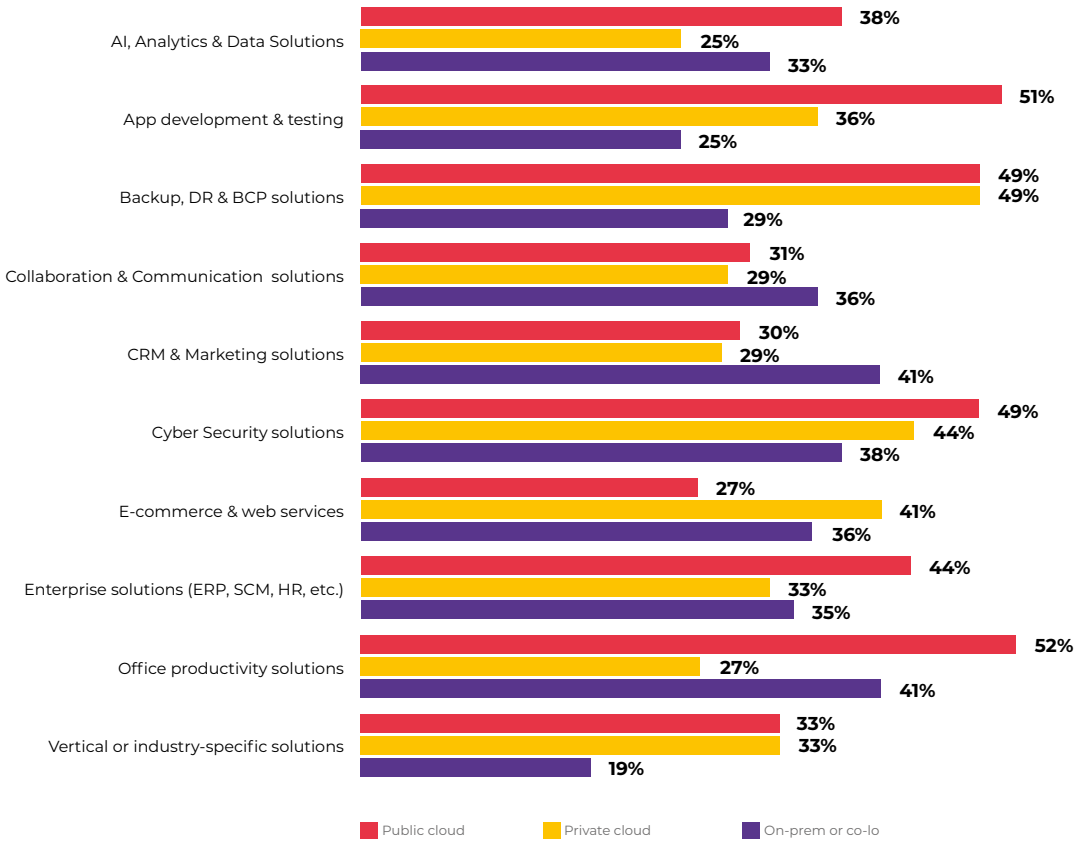

Figure 32: SaaS-first productivity and public-hosted web apps contrast with hybrid or on-prem workloads for core and vertical solutions.

Current Hosting Patterns Across App Categories

Respondents were asked where their key application categories are currently hosted. The results show clear patterns:

- 51.8% of office productivity apps are hosted on-premise or in colocation, but 41.1% now reside in the public cloud.
- 49.1% of cybersecurity solutions remain on-prem/co-lo, while 38.2% are now public cloud-based.
- 43.6% of enterprise systems (ERP, SCM, HR) still sit on-prem—but 32.7% are in private cloud, and 34.6% in public cloud—a healthy hybrid.
- Vertical/industry-specific apps are evenly split—33.3% on-prem, 33.3% private, and 18.5% public.
- E-commerce and web apps have the strongest cloud-native tilt, with 41.1% in private cloud and 35.7% in public cloud.

Notably, very few categories are "not relevant"—indicating broad adoption across enterprise types.

What's Driving These Patterns

- **Public Cloud Finds Its Footing in User-Centric and External Apps** Web, collaboration, and office productivity tools are leading cloud adoption—driven by user demand, SaaS maturity, and ease of migration.
- **Core Systems Are Getting Cloud-Ready—But Gradually** ERP and industry-specific apps are moving cautiously toward cloud, often via replatforming or private deployments first.
- **Security Still Anchored On-Prem** Legacy controls, regulatory concerns, and performance requirements mean many cybersecurity tools remain grounded in traditional environments.

CIO Action Agenda

- Maintain a dynamic hosting strategy based on application criticality, performance, compliance, and integration complexity.
- Modernize core systems through phased migration—beginning with private cloud readiness or hybrid deployments.
- Assess end-user and developer apps for rapid cloud enablement—especially where elasticity and external access add value.
- Re-evaluate security architectures to balance control with cloud-readiness—especially in identity, monitoring, and endpoint defense.

Key Insight

Hybrid is the default for enterprise IT. While public cloud is growing fast—especially for web-facing and collaborative workloads—many core and vertical apps remain rooted in on-premise or private environments.

Takeaways for Ecosystem Partners

- **Cloud providers** should tailor value propositions based on workload type—not just vertical.
- **SIs and platform partners** can help enterprises manage hybrid complexity through tooling, observability, and governance.
- **ISVs and SaaS providers** must continue verticalizing and modularizing offerings to enable easier migration from on-prem roots.

Bottom Line

Application hosting in 2025 is a strategic balancing act. CIOs aren't just choosing platforms—they're sequencing transitions, aligning with business rhythms, and managing risk. Success lies in flexibility, not absolutism.

CLOUD PRACTICES IN PLAY: SAAS AND IAAS LEAD, DEVOPS AND APIS MATURING

Cloud is no longer just about where workloads run—it's about how they're built, delivered, and secured. The 2025 SoT survey reveals high adoption of foundational models like SaaS and IaaS, with increasing maturity in supporting disciplines like DevOps, APIs, and cloud-native architectures.

The core of cloud usage has stabilized. The next leap is about how well enterprises automate, orchestrate, and optimize.

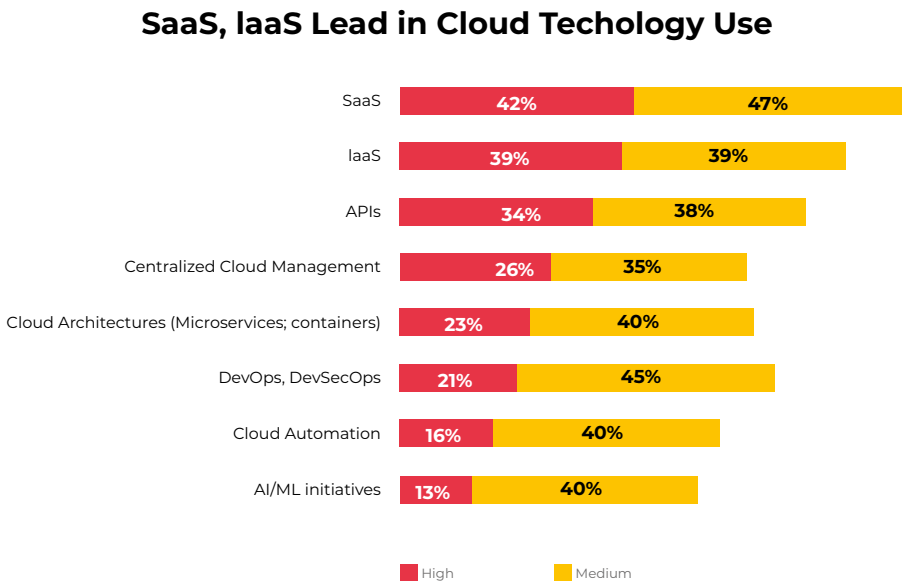

Figure 33: SaaS is nearly universal, IaaS and APIs widely adopted—DevOps and microservices growing steadily.

What's Widely Used—and What's Catching Up

Respondents rated their adoption of key cloud-related technologies and practices. The combined share of "High" and "Medium" usage paints a maturity curve:

- **89.1% report strong adoption of SaaS,** with nearly half (41.8%) rating it "High."
- **77.8% are using IaaS effectively,** with 38.9% reporting it at high maturity.
- **71.4% say APIs are in regular use,** though only 33.9% rate their maturity as "High."
- **66.0% are using DevOps/DevSecOps,** suggesting broad—but still uneven—practice adoption.
- **62.3% are leveraging microservices and**

containers, showing momentum in architecture modernization.
- **Cloud automation and AI/ML workloads,** by contrast, show greater fragmentation, with high shares of "Low" usage or "Not Relevant" responses.

Why This Progression Makes Sense

- **SaaS is the Default Delivery Model** Nearly every enterprise touches SaaS—from collaboration tools to ERP modules—making it the most mature layer.
- **IaaS Remains the Workhorse** Infrastructure-as-a-Service powers modernization, migration, and scalability—especially for legacy and custom workloads.
- **DevOps is Becoming Table Stakes** While not yet universal, DevOps is central to agility. High-medium adoption suggests most enterprises are on the path, if not fully there.
- **APIs Signal Modular Thinking** API maturity is a strong indicator of cloud-native mindset—but governance and lifecycle management still need attention.

66% expect AI to optimize cloud orchestration and cost efficiency—AI isn't just hosted in the cloud, it's improving how the cloud works.

CIO Action Agenda

- Benchmark current cloud practice maturity—not just adoption—and identify gaps in automation, integration, and security.
- Scale DevOps beyond tech teams—infuse into release management, compliance, and operations.
- Strengthen API strategy with versioning, analytics, and developer enablement programs.
- Prioritize automation capabilities that span build, deploy, monitor, and remediate cycles.

Key Insight

The foundation of cloud is firmly in place across Indian enterprises. The next opportunity lies in how well organizations embed automation, modularity, and secure DevOps practices to scale value creation.

Takeaways for Ecosystem Partners

- **Vendors** should shift from enablement to enhancement—helping customers optimize cloud practices, not just adopt them.
- **Consultants and trainers** can drive DevOps, API governance, and microservices skills across mixed-maturity teams.
- **Policy and industry bodies** should support open standards, secure APIs, and enterprise-scale automation benchmarks.

Bottom Line

The cloud journey is no longer about access—it's about execution. Enterprises that move beyond infrastructure to embrace modularity, automation, and intelligence will lead not just in cost savings—but in speed, innovation, and resilience.

TOP CONCERNS: SECURITY, COST, AND CONTINUITY RISE TO THE FORE

As enterprises scale their cloud and digital ambitions, the supporting infrastructure must evolve. The 2025 SoT survey shows that Indian CIOs are laser-focused on security, cost control, and continuity—but also increasingly concerned about infrastructure visibility, automation, and technical debt.

Modern IT infrastructure is no longer just about uptime—it's about resilience, intelligence, and agility under pressure.

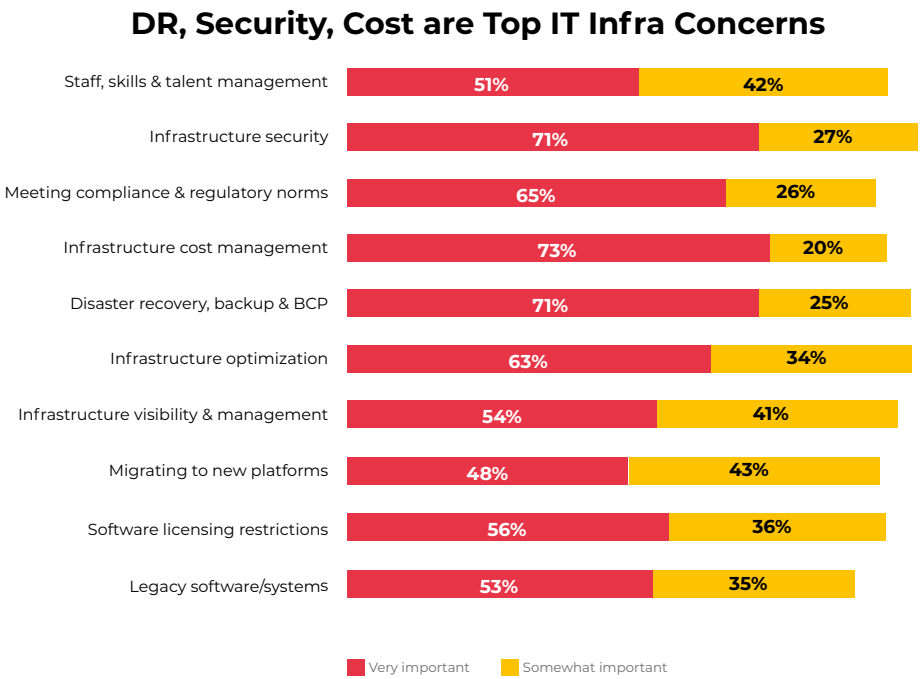

Figure 34: Security and cost dominate infra priorities—visibility, optimization, and resilience also critical.

Which Concerns Rank Highest?

Respondents rated their infrastructure concerns by importance. Here's how they scored:

- **72.7% rate "Infrastructure cost management" as very important,** with another 20.0% saying it's somewhat important.
- **70.9% flagged "Infrastructure security" and "Disaster recovery, backup & BCP"** as very important.
- **62.5% prioritized "Infrastructure optimization"

for performance, efficiency, and automation gains.
- **53.6% flagged "Infrastructure visibility & management" as very important, but 41.1% said it was somewhat important—**signaling broader recognition.

Lower down the list, concerns like **migration to new platforms** and **legacy software** were still notable but slightly less urgent in the current cycle.

What the Rankings Reveal

- **Security and Resilience Are Non-Negotiable** With rising threats and regulatory scrutiny, security and business continuity have become core CIO responsibilities—not just IT functio**ns.**
- **Cost Pressure Is Real—and Rising** As cloud bills and hybrid infrastructure complexity mount, CIOs are doubling down on spend visibility and optimization levers.
- **Visibility and Governance Lag Behind** Despite tooling advancements, many enterprises still lack end-to-end observability across cloud, data center, and edge environments.
- **Legacy Drag Remains a Friction Point** Although not at the very top, legacy systems and software still constrain modernization speed and architecture alignment.

> Legacy drag and visibility gaps still hinder progress, demanding sharper governance and optimization.

CIO Action Agenda

- Prioritize cost transparency across cloud and on-prem through unified dashboards and FinOps practices.
- Strengthen infra security posture through zero-trust models, automated patching, and multi-cloud visibility.
- Revisit disaster recovery plans to reflect hybrid realities—including SaaS and IaaS dependencies.
- Invest in observability platforms that span infrastructure, applications, and user experience.

Key Insight

The infrastructure conversation is shifting from capacity to capability. CIOs want environments that are secure, scalable, cost-efficient—and built for failure and rapid recovery.

Takeaways for Ecosystem Partners

- **Vendors** should bundle visibility, cost optimization, and DR automation into core offerings—not just premium tiers.
- **Consultants and SIs** must help enterprises move from infra operations to infra intelligence—especially across multi-cloud.
- **Toolmakers** should build for cross-environment consistency, policy enforcement, and stakeholder visibility.

Bottom Line

Modern infrastructure must deliver more than just uptime. The enterprises that treat it as a strategic enabler—not just a backend utility—will unlock new agility, resilience, and innovation capacity.

WHY CLOUD NOW? INNOVATION AND EXPERIENCE TRUMP COST

Once championed primarily for its elasticity and cost advantage, cloud is now central to enterprise innovation and transformation. The 2025 SoT survey reveals a clear pivot in enterprise priorities: CIOs see cloud as a catalyst for business change, not just a platform upgrade.

Enterprises are moving from cloud for IT efficiency to cloud for strategic agility.

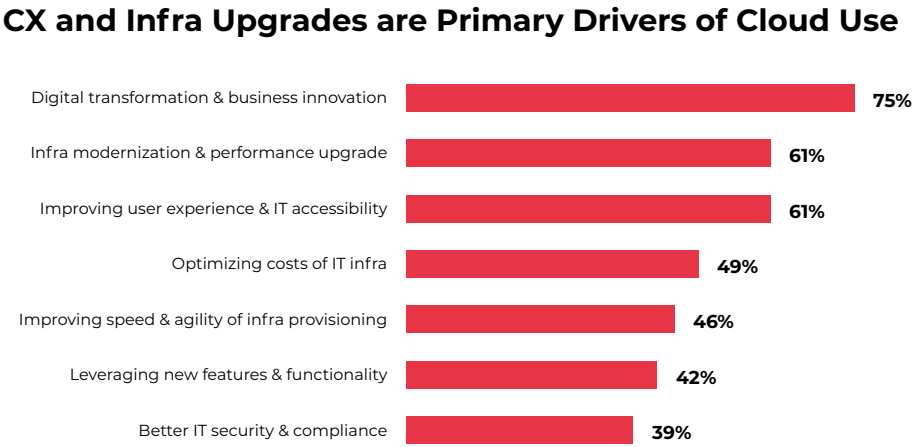

Figure 35: Cloud adoption drivers shift from cost savings to transformation, agility, and user-centric value.

Top Drivers for Cloud Investments in the Next 12 Months

When asked about the primary reasons for expanding cloud usage in the year ahead, CIOs pointed to a mix of strategic, operational, and experiential goals:

- **75.4% chose "Digital transformation and business innovation"—**making it the single strongest motivator.
- **61.4% each cited "Improving user experience & IT accessibility" and "Infra modernization & performance upgrades."**
- **49.1% are focused on "Optimizing costs of IT infrastructure."**
- **45.6% are looking to "Improve speed and agility of infra provisioning."**
- **42.1% want access to "New features and functionality."**
- **38.6% aim to "Improve IT security and compliance."**

This mix underscores that cloud is no longer a back-end decision—it's a business enabler.

Decoding the Shift in Priorities

- **Cloud = Change Platform** Enterprises

increasingly see cloud as the foundation for business model shifts, innovation programs, and digital products.

- **User Experience Is Now a Core Metric** Cloud is being leveraged to simplify access, reduce latency, and enhance responsiveness—especially in hybrid work and customer-facing environments.
- **Infra Speed Matters—But So Does Sustainability** Faster provisioning, automation, and scalability remain important—but they now support broader transformation narratives.
- **Cost is a Consideration, Not the Core** While cost optimization still matters, it's no longer the dominant or sole driver of cloud momentum.

CIO Action Agenda

- Reposition cloud programs as innovation and experience enablers—not just efficiency plays.
- Link cloud KPIs to user satisfaction, business velocity, and digital maturity—not just uptime or cost.
- Create cross-functional initiatives that leverage cloud capabilities to accelerate transformation agendas.
- Educate internal stakeholders on the strategic potential of cloud beyond infrastructure.

Key Insight

Cloud is becoming a boardroom topic—not just a CIO concern. The drivers have expanded from IT outcomes to business relevance, innovation potential, and user-centric performance.

Takeaways for Ecosystem Partners

- **Cloud vendors** must speak the language of innovation, agility, and transformation—not just capacity and savings.
- **Consultants and integrators** should help CIOs craft cloud narratives that align with CEO and business unit goals.
- **SaaS and PaaS providers** must demonstrate how features and scalability unlock new customer experiences.

> Cloud isn't just the destination—it's the engine of transformation. CIOs who tie cloud strategy to business reinvention will drive greater impact and influence.

Bottom Line

Cloud is no longer just the "where"—it's increasingly the "how" behind transformation. CIOs who align their cloud roadmap with business reinvention will earn greater strategic credibility—and deliver outsized impact.

CLOUD CHALLENGES: COST, TALENT, AND MONITORING DOMINATE THE ROADBLOCKS

While cloud momentum continues across Indian enterprises, the road to value creation is increasingly shaped by nuanced challenges. The 2025 SoT survey reveals that financial sustainability, operational complexity, and skill gaps have emerged as the biggest obstacles to seamless cloud adoption.

The message from CIOs is clear: scaling cloud isn't the hard part—scaling it right is.

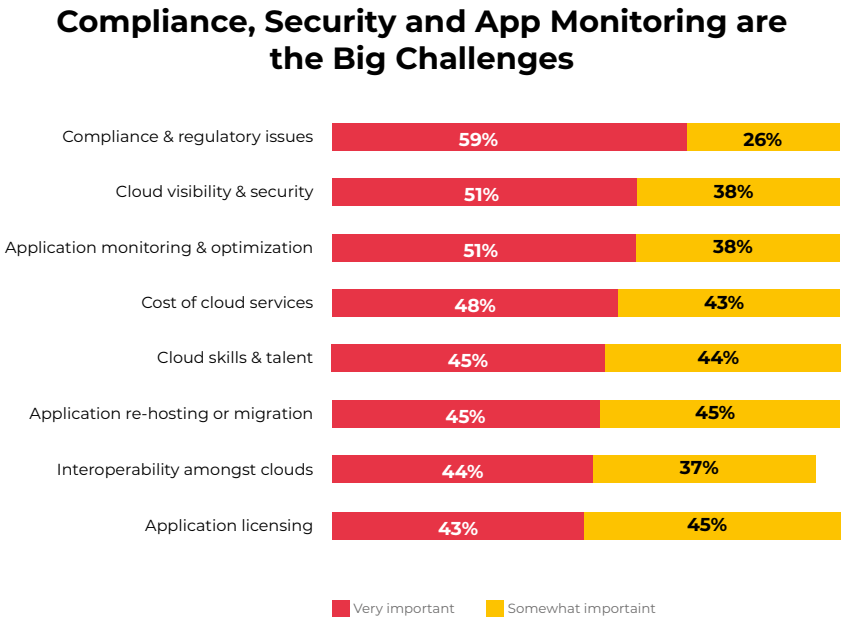

Figure 36: Cloud strategy is being reshaped by financial vigilance, migration friction, and visibility demands.

Top Challenges Facing Cloud Initiatives

Respondents rated their most pressing cloud challenges by level of importance. Here's where the biggest blockers lie:

- **91.1% of CIOs cite "Cost of cloud services" as a key concern, with 48.2% rating it** very important.
- **89.3% say "Application re-hosting or migration" is a critical hurdle,** due to complexity and legacy dependencies.
- **89.1% each call out "Cloud skills & talent," "Application monitoring & optimization," and "Cloud visibility & security"** as very or somewhat important.

Other issues such as interoperability, licensing, or vendor lock-in were also mentioned but ranked slightly lower in urgency.

Interpreting the Patterns

- **Cloud Economics is in Focus** As workloads scale, many enterprises are hitting unexpected cost ceilings—triggering a shift toward FinOps, right-sizing, and usage control.
- **Migration Isn't Plug-and-Play** Moving legacy apps to the cloud often requires more than rehosting—it demands re-architecture, dependency untangling, and re-integration.
- **Talent is a Pacing Constraint** Skill shortages in cloud engineering, DevOps, and security are stalling execution—even in enterprises with clear intent.
- **Visibility and Control Gaps** Many organizations lack the tools or processes to monitor performance, enforce policies, or detect anomalies across multi-cloud environments.

> To turn cloud into a business lever, CIOs must sharpen cost visibility, optimize workloads, retain talent, and ensure full-stack observability.

CIO Action Agenda

- Prioritize cost observability with real-time dashboards, tagging policies, and cloud budgeting tools.
- Triage migration workloads—separating rehost candidates from those requiring full modernization.
- Invest in cloud talent retention and cross-training while partnering for specialist capabilities.
- Strengthen observability and monitoring to reduce latency, sprawl, and blind spots across environments.

Key Insight

The cloud journey is no longer about enthusiasm—it's about discipline. Cost, control, and capability now define the success of cloud strategy far more than infrastructure availability or vendor maturity.

Takeaways for Ecosystem Partners

- **Cloud providers** must prioritize pricing transparency, granular billing, and predictive analytics.
- **Service providers and integrators** should offer migration tooling, refactoring templates, and talent augmentation.
- **Security and monitoring platforms** must support multi-cloud telemetry, alerting, and compliance automation.

Bottom Line

The cloud story is evolving from expansion to optimization. CIOs who actively manage costs, talent, and operational transparency will gain far more than scalability—they'll unlock sustained business value.

NEXT FOR CLOUD: OPTIMIZATION, EDGE, AND API INTEGRATION

Cloud has entered a phase of purposeful growth. The 2025 SoT survey shows that Indian enterprises are no longer just migrating workloads—they're refining them. Over the next 12 months, cloud priorities are pivoting from migration to optimization, with cost, performance, and architecture shaping the new agenda.

Cloud isn't shrinking—it's evolving.

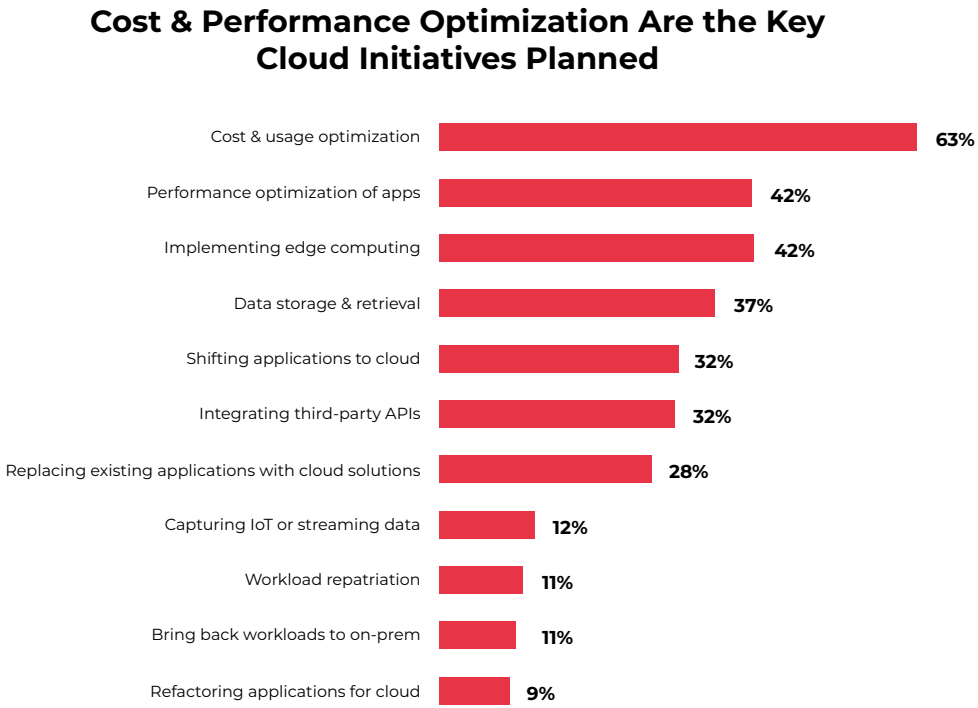

Figure 37: Enterprises shift focus to cost control, performance tuning, and distributed computing—repatriation enters the mix.

What Cloud Initiatives Are on the Horizon?

CIOs shared their planned cloud initiatives for the coming year. Here's what ranked highest:

- **63.2% will prioritize "Cost and usage optimization."**
- **42.1% plan to adopt "Edge computing."**
- **42.1% also aim to drive "Performance**

optimization of cloud applications."

- **36.8% will focus on "Data storage and retrieval" enhancement.**
- **31.6% will work on "Integrating third-party APIs."**
- **21.1% are considering "Refactoring apps for cloud"—a deeper modernization step.**
- **Around 10.5% plan "Workload repatriation" or "bringing workloads back on-prem," signaling early cost or performance concerns.**

These priorities reflect a blend of technical fine-tuning, architectural evolution, and selective realignment.

What These Initiatives Suggest

- **Cloud Optimization Is a Strategic Priority** With costs rising and budgets tightening, CIOs are scrutinizing usage, right-sizing workloads, and enhancing cloud governance.
- **Edge is Entering the Mainstream** As data and compute decentralize, edge is gaining traction for latency-sensitive, real-time, or field applications.
- **Performance Over Raw Scale** Optimization of existing apps—not just spinning up new ones—is becoming a key value lever.
- **Selective Repatriation Is Real—but Not Dominant** Some enterprises are reassessing cloud workloads due to unexpected cost, complexity, or compliance constraints.

> CIOs must drive FinOps, align to SLAs, treat APIs strategically, tap the edge when needed, and plan for hybrid with repatriation readiness.

CIO Action Agenda

- Launch or mature FinOps practices to govern cost, utilization, and forecasting.
- Evaluate edge architectures where latency, bandwidth, or autonomy are critical.
- Benchmark cloud app performance against business SLAs—optimize accordingly.
- Treat API integration as a strategic capability—not just a technical task.
- Document and de-risk repatriation plans if exploring hybrid realignment.

Key Insight

The cloud narrative is shifting from migration to maturity. Optimization, edge-readiness, and selective modernization are the new themes guiding enterprise roadmaps.

Takeaways for Ecosystem Partners

- **Cloud providers** must double down on tooling for observability, usage analytics, and edge orchestration.
- **Consultants** can help organizations refactor strategically—balancing performance, portability, and cost.
- **Platform vendors** should strengthen support for hybrid, edge, and modular APIs to meet evolving architectures.

Bottom Line

Cloud is no longer the destination—it's the platform for continuous transformation. Enterprises that refine, not just expand, their cloud strategies will achieve greater agility, efficiency, and resilience.

MODERNIZING THE DATA CENTER: HYPERCONVERGENCE AND SUSTAINABILITY RISE

Even as cloud adoption surges, Indian enterprises are not abandoning their on-premise and colocation environments. Instead, they're modernizing them. The 2025 SoT survey reveals that hyperconverged infrastructure, energy-efficient design, and software-defined platforms are key focus areas—while interest in bringing workloads back from cloud remains cautious and selective.

The data center's role is shifting—from bulk infrastructure to specialized, optimized infrastructure.

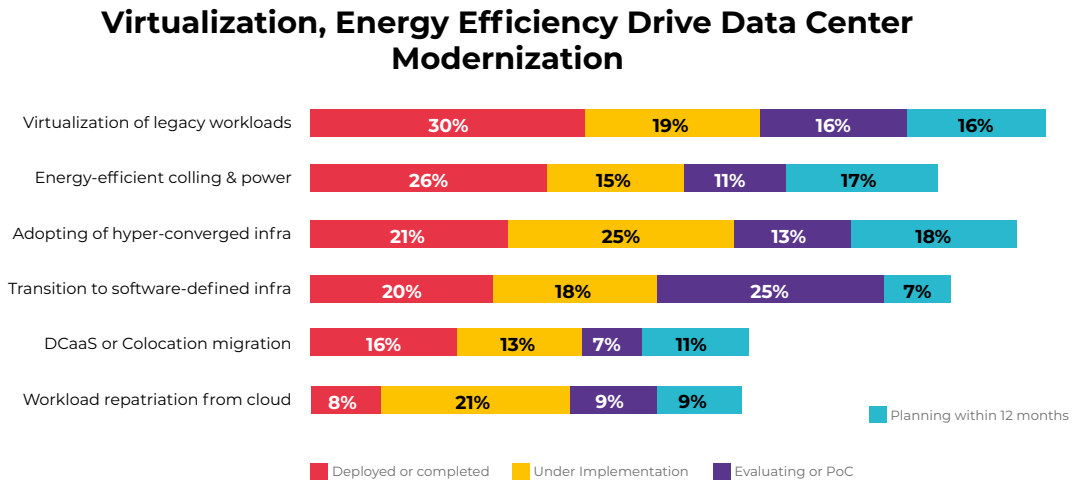

Figure 38: Enterprises are pushing ahead with software-defined infra, HCI, and green datacenter initiatives—repatriation a minor trend.

What Are Enterprises Modernizing in Their Data Centers?

Respondents shared their current and planned data center modernization initiatives. Here's what stood out (based on weighted average across evaluation, implementation, and deployment):

- **DCaaS and Colocation Migration** tops the list with the highest weighted average of 3.89, reflecting demand for flexibility without full cloud commitment.
- **Workload Repatriation from Cloud** sees moderate interest (3.75), though mostly in evaluation or partial implementation stages.
- **Energy-efficient cooling and power systems** have a score of 3.43, driven by cost and sustainability mandates.
- **Adoption of Hyper-Converged Infrastructure (HCI)** ranks at 3.14, reflecting continued architectural consolidation.
- **Software-defined infrastructure transitions**

show mixed progress, largely in evaluation or planning.

While most initiatives are still in early or mid-stage rollout, the trend is clear: enterprises want more agility, visibility, and sustainability from their on-prem investments.

What These Patterns Suggest

- **DCaaS Gains Favor as a Cloud Bridge** Colocation and DCaaS models offer flexibility, reduced capital expense, and proximity to cloud on-ramps—making them attractive to hybrid adopters.
- **Repatriation Is Real—But Limited** A small but visible set of enterprises are re-evaluating cloud placements for cost, latency, or control reasons.
- **Green Infra Is a Priority** Energy efficiency is rising up the agenda—not just for ESG goals, but also for operating cost reduction.
- **HCI Adoption Reflects Simplification Goals** Consolidating compute, storage, and networking into a single platform is appealing—especially for mid-size enterprises and edge setups.

87% of enterprises cite digital innovation as the primary reason for continued cloud investments, highlighting cloud's central role in enabling AI, faster application development, and agile business models.

CIO Action Agenda

- Build a decision matrix to guide app placement across cloud, colocation, and DCaaS.
- Evaluate repatriation only where there's a clear cost-performance or regulatory upside.
- Prioritize DC optimization initiatives that deliver tangible ROI—especially in power, cooling, and automation.
- Invest in software-defined tooling that improves infra manageability and provisioning agility.

Key Insight

The data center isn't going away—it's being refactored. Enterprises want it leaner, greener, and more responsive to cloud-era expectations.

Takeaways for Ecosystem Partners

- **Colocation and DCaaS providers** must align offerings with hybrid and edge demands—ensuring connectivity, scalability, and governance.
- **Infra OEMs and software vendors** should accelerate roadmaps for HCI, energy monitoring, and software-defined management.
- **Integrators** can lead modernization programs that blend refactoring with sustainability and cost optimization.

Bottom Line

The future of the data center is not about footprint—it's about function. CIOs who treat it as a strategic asset—not just a cost center—will future-proof infrastructure in a hybrid, AI-driven world.

READYING FOR AI: ORCHESTRATION, MLOPS AND ON-PREM COMPUTE LEAD THE STACK

AI needs more than data and models—it needs an optimized, flexible, and cost-aware infrastructure layer. The 2025 SoT survey shows that Indian enterprises are taking foundational steps to ready their environments for AI/ML workloads. From workload orchestration to MLOps pipelines and selective on-prem GPU deployments, the focus is on control, scalability, and manageability.

AI infrastructure readiness is not about raw power—it's about integration, visibility, and long-term scalability.

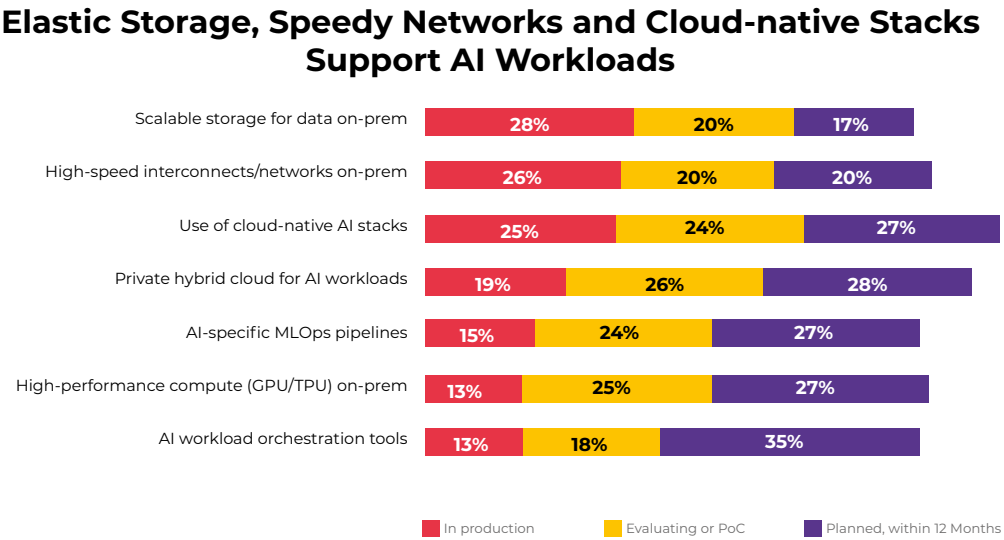

Figure 39: AI infrastructure plans show a blend of orchestration tooling, pipeline enablement, and selective GPU/TPU investments.

Where Enterprises Are Investing in AI Infra Readiness

Respondents identified their current status across various AI infrastructure initiatives. Ranked by weighted average, here's what stands out:

- **AI workload orchestration tools top the list (2.85 weighted avg), with over 34.6% planning to deploy in the next 12 months.**
- **AI-specific MLOps pipelines** follow closely (2.73), showing strong evaluation and planning interest.
- **On-prem high-performance compute (GPU/TPU)** ranks at 2.71, with more than 25% evaluating or implementing**.**
- **High-speed on-prem interconnects and**

networking come in slightly lower (2.67), but signal important groundwork.

Across all these areas, nearly **1 in 3 enterprises still report no plans,** revealing a wide maturity spectrum in AI readiness.

What This Data Tells Us

- **Control and Coordination Matter More Than Just Hardware** Enterprises are prioritizing orchestration and MLOps pipelines ahead of brute-force compute—showing a preference for manageable, scalable infrastructure.
- **On-prem GPU Investments Are Selective** While public cloud remains a strong option for training workloads, some organizations want on-prem compute for privacy, control, or latency reasons.
- **Readiness is Patchy but Growing** Most AI infra initiatives are in PoC or planning stages—indicating momentum but also caution.

> Enterprises are ramping up AI infrastructure with a focus on workload orchestration, MLOps pipelines, and on-prem GPU deployments.

CIO Action Agenda

- Evaluate orchestration and MLOps tools for standardization, automation, and governance in AI pipelines.
- Build AI infrastructure planning into your broader hybrid cloud strategy—considering cost, performance, and data gravity.
- Invest in cross-functional collaboration between data science and infrastructure teams to align needs.
- Consider edge AI infra use cases where latency or privacy demands local compute power.

Key Insight

AI infrastructure maturity starts with orchestration, not hardware. CIOs are investing in control layers and pipelines before scaling compute—which will enable sustainable AI growth across the enterprise.

Takeaways for Ecosystem Partners

- **Platform vendors** must support AI orchestration and MLOps with modular, open, and hybrid-ready tools.
- **Infra providers** should tailor GPU, HCI, and networking offerings for AI-specific use cases—not generic deployments.
- **Consultants** can help design infra blueprints for AI across industries—from pilots to scale-up.

Bottom Line

The winners in AI won't just be the ones with the biggest GPUs—they'll be the ones with the smartest pipelines. Enterprises that prioritize flexibility, orchestration, and integration will be best placed to operationalize AI at scale.

CLOUD'S BUSINESS IMPACT: INNOVATION, PERFORMANCE, AND PRODUCTIVITY

Cloud's value narrative has matured. No longer just a lever for IT cost savings, it's now seen as a platform for delivering new products, improving application performance, and strengthening resilience. The 2025 SoT survey reveals that Indian enterprises are realizing tangible business benefits across innovation, user experience, and operations.

The cloud payoff is increasingly measured in speed, scale, and service, not just in savings.

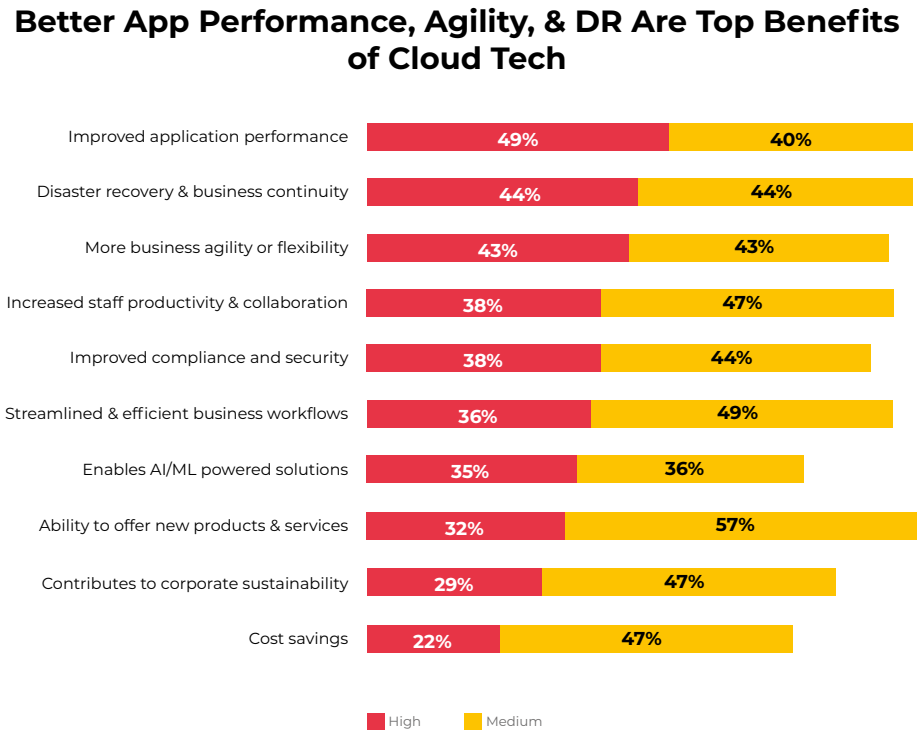

Figure 40: Cloud enables product agility, application performance, and business continuity—cost savings ranked modest.

What Are the Most Valued Cloud Outcomes?

Respondents ranked business benefits from their cloud investments. The combined share of "High" and "Medium" impact reveals where cloud is making the biggest difference:

- **89.3% said cloud enables "Offering new products and services,"** with over 32% rating it as highly impactful.

- **89.1% highlighted "Improved application performance."**
- **88.9% credited cloud for enhancing "Disaster recovery and business continuity."**
- **85.5% reported gains in "Business workflow efficiency" and "Staff productivity."**
- **Only 69.1% rated "Cost savings" as high or medium impact,** with just 21.8% calling it a top-tier outcome.

This distribution shows that the business case for cloud now rests on outcomes beyond operational cost.

Decoding the Benefits Curve

- **Innovation Over Infrastructure** Enterprises are using cloud platforms to launch digital services faster—especially in customer-facing functions.
- **Performance and Reliability at Scale** Faster response times, uptime assurance, and scalable infrastructure are driving business confidence.
- **Cloud as a Productivity Multiplier** Collaboration, mobility, and real-time access are powering distributed teams and process simplification.
- **Cost Matters—But Isn't the Main Event** With growing usage and complexity, cloud costs are being managed—but aren't always the core benefit.

> Ethical AI in the cloud is slow to rise—only 52% expect adoption within two years, revealing a trust gap in enterprise AI plans.

CIO Action Agenda

- Quantify cloud success through business-facing KPIs—time-to-market, user NPS, product velocity—not just infra metrics.
- Partner with business units to identify innovation-led cloud use cases—especially in product, sales, and CX.
- Reassess legacy cost-focused cloud narratives to reflect agility, experience, and resilience benefits.
- Build performance observability into cloud-native environments to align ops with end-user satisfaction.

Key Insight

Cloud is becoming a platform for reinvention—not just a delivery model. The business benefits most appreciated today reflect agility, speed, and service quality.

Takeaways for Ecosystem Partners

- **Cloud vendors** should anchor conversations in business value—industry use cases, product agility, and customer impact.
- **Advisors and integrators** must help align IT and business goals to realize the full cloud potential.
- **Tooling providers** can support performance monitoring, user experience metrics, and business-aligned observability.

Bottom Line

Cloud is paying off—but not always in the ways enterprises first expected. CIOs who align cloud strategy with business reinvention will maximize both value and visibility.

AI-IN-CLOUD INNOVATIONS: OPTIMIZATION AND ORCHESTRATION LEAD EXPECTATIONS

As enterprises deepen their use of AI and cloud together, expectations are rising around AI-native cloud features. The 2025 SoT survey reveals that Indian CIOs are most bullish on operational AI—tools that optimize infrastructure, automate orchestration, and enhance visibility. Meanwhile, areas like ethical AI governance and privacy controls are seen as longer-term priorities.

AI-in-cloud isn't just about smarter apps—it's about a smarter stack.

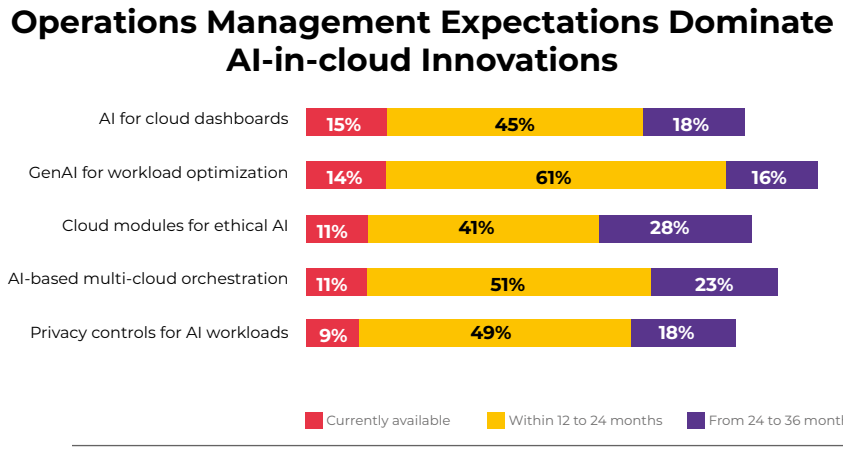

Figure 41: GenAI-driven workload tuning, AI dashboards, and multi-cloud orchestration top the wish list—ethical AI and privacy tools still further out.

Which Innovations Are Expected First?

Respondents were asked when they expect specific AI-driven innovations to become enterprise-ready. Ranked by those who believe capabilities are available now or within the next 24 months, here's what stands out:

- **75.0% expect "GenAI for workload optimization" within 24 months,** with 14.3% saying it's already available.
- **61.4% anticipate "AI-based multi-cloud orchestration"** in that same window.
- **60.0% are looking forward to "AI for cloud dashboards",** particularly in observability and ops.
- 58.2% foresee "Privacy controls for AI workloads" emerging in the near term.
- **Only 51.9% expect "Cloud modules for ethical AI" in that time frame,** with a significant share pushing it out beyond 2 years.

The data shows that immediate expectations are tied to infrastructure efficiency and monitoring—while governance and compliance innovations will take longer to mature.

What These Signals Tell Us

- **Optimization First, Ethics Later** CIOs are prioritizing AI that drives operational efficiency—before turning to frameworks for ethical or

privacy-sensitive AI deployment.

- **AI at the Infra Layer is Maturing** Multi-cloud orchestration and AI-powered dashboards reflect a growing appetite for automation and autonomous cloud management.
- **Governance Is Still Gaining Mindshare** While ethical and privacy controls are important, they're seen as aspirational or externally driven—rather than near-term operational mandates.

> Cloud's real value is emerging beyond cost savings or scalability. CIOs who align cloud with business reinvention—not just migration—are unlocking greater impact, agility, and strategic visibility.

CIO Action Agenda

- Evaluate GenAI and AI-based optimization tools embedded within cloud platforms—especially for workload sizing, auto-scaling, and anomaly detection.
- Monitor advancements in AI-driven dashboards and orchestration layers—prioritize pilots in multi-cloud or hybrid environments.
- Collaborate with legal and compliance teams to prepare for future expectations around privacy-preserving AI and ethical guardrails.
- Stay close to vendor roadmaps on AI governance tooling—regulatory timelines may accelerate needs.

Key Insight

AI's next frontier is infrastructure intelligence. The most immediate value lies in making cloud smarter—before tackling more complex ethical or regulatory use cases.

Takeaways for Ecosystem Partners

- **Cloud and platform vendors** must double down on embedded GenAI and orchestration capabilities—making them easy to adopt, monitor, and optimize.
- **Tooling providers** should focus on visibility, cost intelligence, and automation as early use cases.
- **Policy and standards bodies** can drive momentum on ethical and privacy-enabling modules for cloud-based AI—creating frameworks CIOs can adopt quickly.

Bottom Line

The future of AI in cloud isn't just about building apps—it's about building intelligence into the very fabric of cloud infrastructure. CIOs who embrace these capabilities early will unlock better agility, performance, and trust.

IT Security
Building Resilience in a Hyper-exposed World

As threats grow more intelligent and pervasive, Indian enterprises are reshaping their security playbooks—investing in automation, talent, and zero-trust frameworks to stay secure, agile, and compliant.

Contents

Executive Summary

In 2025, cybersecurity has emerged not just as an operational necessity, but as a strategic foundation for enterprise trust. Indian organizations are contending with a diverse threat landscape—where phishing (55%), identity-based attacks (46%), and ransomware (38%) top the list of high-severity risks. The fallout is equally stark: nearly one-fourth of the respondents report business disruptions, data loss, or financial damage from recent incidents.

Nevertheless, the response is maturing. Enterprises are embracing AI-powered security operations, investing in cloud-native controls, and retraining talent at scale. Over 64% are retraining technical staff, while 59% are actively working with expert partners to bridge skill gaps. Incident response and IT/network monitoring are now the top areas for AI deployment, with over 83% expecting significant impact within 18 months.

IAM and privacy practices are gaining maturity. Nearly 68% have deployed or are implementing Privacy Impact Assessments, while identity governance is expanding through multi-factor authentication and privileged access controls.

Still, challenges persist. Cloud security misconfigurations, lack of unified visibility, and AI-related risks—including deepfakes, model poisoning, and data leakage—are creating new layers of vulnerability. Notably, 93% of enterprises express concern over AI misuse in cybersecurity.

In this context, security is no longer a standalone function—it is being embedded across cloud, apps, infrastructure, and data workflows. CIOs and CISOs are building not just defense, but resilience by design.

The intelligent enterprise of 2025 treats trust as both a differentiator and a discipline—one where strategy, tooling, and talent evolve together to meet a shifting risk landscape.

PHISHING AND MALWARE TOP THE THREAT CHARTS

Indian enterprises are contending with a widening threat spectrum—from the familiar (phishing, malware) to the insidious (APTs, zero-days). The 2025 SoT survey reveals that phishing attacks continue to dominate in terms of severity, with nearly 77% of respondents rating them as highly or moderately severe. Malware, identity-based threats, and zero-day exploits also emerged as high-concern areas, confirming that enterprises are under constant siege across multiple vectors.

The message is clear: today's security leaders must defend across both depth and breadth.

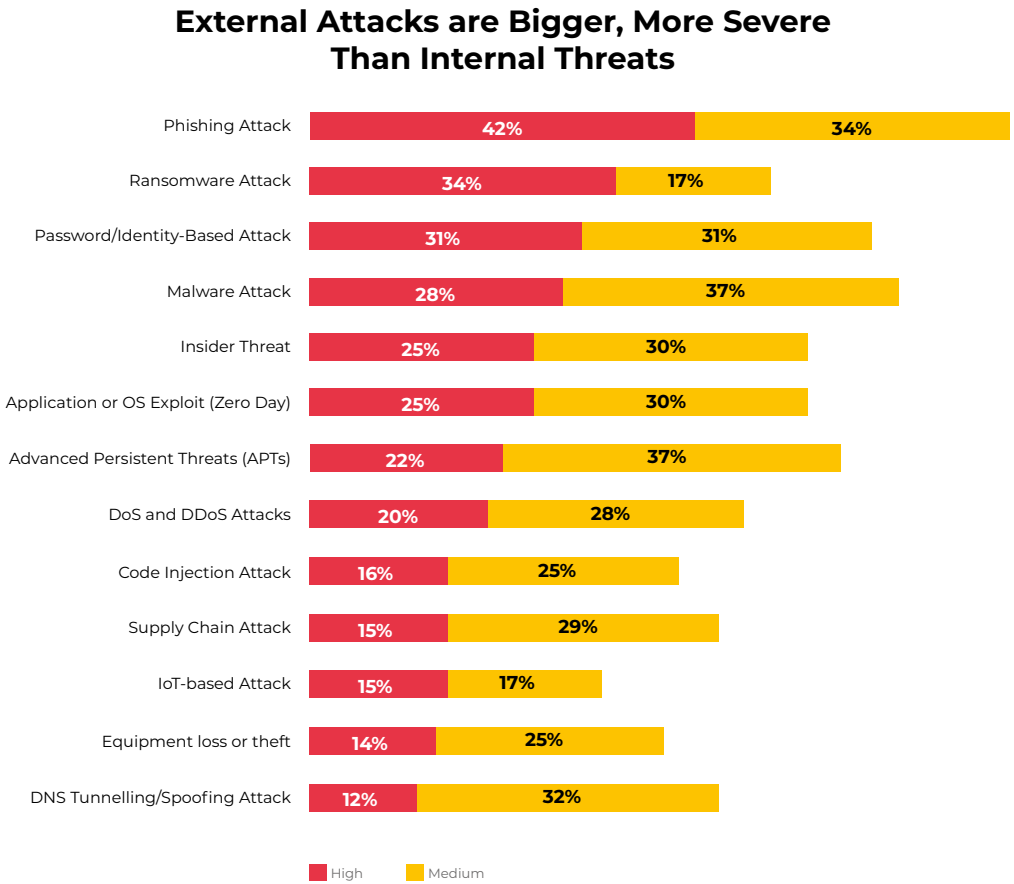

Figure 42: Phishing ranks highest in perceived severity, with malware and identity-based attacks close behind.

Top Security Threats by Perceived Severity

CIOs and CISOs rated a wide range of attack types based on how severe they've been over the past year. Key highlights:

- **76.6% ranked phishing attacks as high or medium severity,** making it the most widespread and impactful category.
- **64.6% cited malware attacks,** reinforcing their continued relevance in the security mix.
- **61.5% marked password/identity-based attacks** as serious threats—reflecting persistent weaknesses in credential hygiene and access controls.
- **58.5% of respondents flagged Advanced Persistent Threats (APTs)** as moderately or highly severe.
- **54.7% called out zero-day application or OS exploits,** indicating growing concern over unknown vulnerabilities.

By contrast, some newer or more niche threats (e.g., IoT attacks, DNS tunneling) were rated lower in severity—either due to limited exposure, or better containment.

What These Findings Reveal

- **Phishing Remains Public Enemy #1** Despite years of awareness efforts, phishing continues to evolve—often powered by GenAI and social engineering finesse.
- **Malware Is a Persistent Drain** Ransomware and fileless malware still hit core systems and endpoints, particularly in under-monitored environments.
- **Identity Is the New Perimeter** Credential-based attacks are growing with cloud adoption and remote work—making IAM and MFA more critical than ever.
- **APTs and Zero-Days Are Rising in Visibility** While less frequent, these sophisticated threats carry disproportionate risk—especially for critical infrastructure and IP-heavy industries.

CIO Action Agenda

- Reinvest in phishing resilience—via simulation, adaptive email protection, and contextual training.
- Strengthen endpoint detection and response (EDR) to catch malware early—especially in distributed workforces.
- Adopt identity-first security frameworks—MFA, Just-in-Time access, and behavioral baselining.
- Expand threat intelligence and zero-day patching capabilities—particularly in DevSecOps and infrastructure teams.

Key Insight

Severity doesn't just track with attack frequency—it reflects business impact, detection gaps, and lateral movement potential. Phishing, malware, and identity threats remain high not because they're novel—but because they still work.

Takeaways for Ecosystem Partners

- **Vendors** must deliver more contextual, behavior-aware phishing protection—and not just signature-based filtering.
- **Managed security providers** can add value through 24/7 SOCs, threat hunting, and breach readiness simulations.
- **Training and awareness partners** should modernize curriculum to reflect AI-generated content, QR scams, and mobile-first phishing.

Bottom Line

The threat landscape is diversifying—but it hasn't moved on from the basics. Enterprises that ignore phishing, identity security, or endpoint hygiene do so at their own peril. Get the fundamentals right—then scale up your threat defense maturity.

INCIDENT IMPACT: BUSINESS DISRUPTION AND BRAND DAMAGE

IT security is no longer just a technology issue—it's a business continuity, reputational, and regulatory risk. The 2025 SoT survey shows that the most commonly felt impacts of cyber incidents are disruption to operations and damage to brand and trust. While data loss and financial impact are also widely reported, it's the business-facing outcomes that dominate the CIO and CISO radar today.

Security failures are measured in downtime, dollars, and damaged credibility.

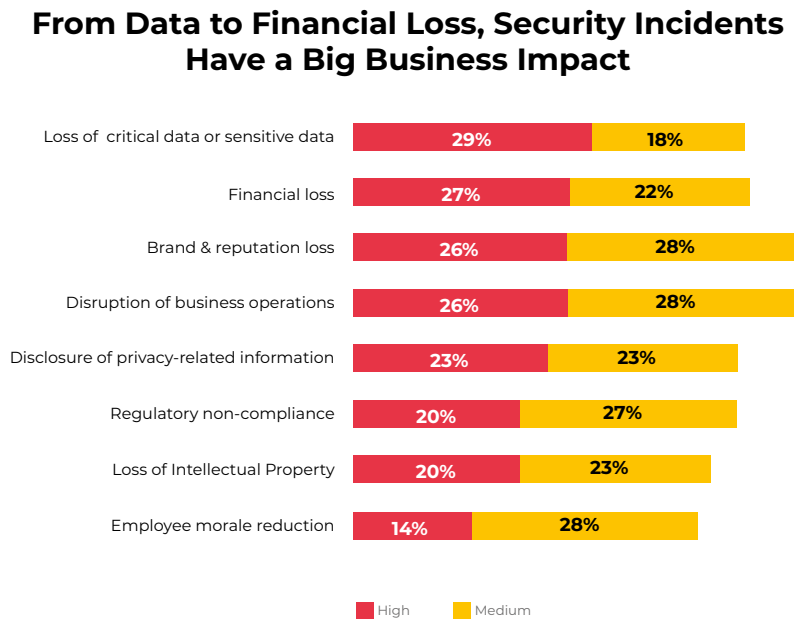

Figure 43: Enterprises report operational disruption, reputation loss, and financial exposure as leading fallout from cyber incidents.

Most Common Consequences of Security Incidents

CIOs rated the organizational impacts of recent security events. Here are the top outcomes by combined high and medium impact ratings:

- **53.8% cited "Disruption of business operations"—**a clear reminder that security downtime equals business downtime.
- **53.8% also flagged "Brand and reputation loss"—**particularly in regulated and consumer-facing industries.
- **48.4% reported "Financial loss,"** with over a quarter rating it as highly significant.
- **47.7% experienced "Loss of critical or sensitive data."**

- **46.9% pointed to "Disclosure of privacy-related information."**

Interestingly, "employee morale," "regulatory non-compliance," and "loss of IP"—while still present—ranked slightly lower in perceived business impact.

Interpreting the Impact Landscape

- **Operational Risk is Front and Center** Whether due to ransomware, DDoS, or insider error—business disruption is the most immediate and visible consequence.
- **Reputational Damage is a Board-Level Concern** In the age of social media, news of breaches spreads fast—and customer trust erodes even faster.
- **Data Loss Has a Double-Edged Effect** Critical data breaches often lead to both financial penalties and long-term credibility damage.
- **Regulatory Risk is Increasing—but Not Yet Top of Mind** As data protection laws strengthen, regulatory impact is expected to rise in future surveys.

> 93% of enterprises say AI misuse in cybersecurity is a high or medium concern—deepfakes, model poisoning, and data leakage are top fears.

CIO Action Agenda

- Elevate cybersecurity from operational shield to business enabler—link investments to uptime, brand equity, and compliance posture.
- Conduct regular tabletop exercises simulating business disruption, data leaks, and reputational fallout.
- Define cross-functional incident response plans—IT, legal, PR, and customer service must be aligned.
- Prioritize detection and containment to minimize downtime and business impact.

Key Insight

The true cost of a security incident isn't just technical—it's commercial. Enterprises that fail to protect critical operations and reputational assets risk far more than just system downtime.

Takeaways for Ecosystem Partners

- **Vendors** should communicate how security solutions support business resilience—not just threat defense.
- **IR and PR specialists** can add value to CISOs by preparing breach communication templates and rehearsal protocols.
- **Policy advisors and compliance consultants** must help enterprises anticipate regulatory escalations and response obligations.

Bottom Line

Security is no longer a back-office risk—it's a boardroom priority. CIOs who build security into business continuity, brand protection, and customer trust will secure more than just their networks—they'll secure their enterprise's future.

SECURITY GAPS: MISCONFIGURATION, HUMAN ERROR, AND INSIDER MISUSE TOP THE LIST

While external threats often dominate headlines, internal missteps remain the most common triggers of security breaches. The 2025 SoT survey reveals that Indian enterprises face more incidents from human error, misconfigurations, and insider actions than from traditional malware or external exploits.

It's not always malicious actors—sometimes it's just a mis-click or a missed setting.

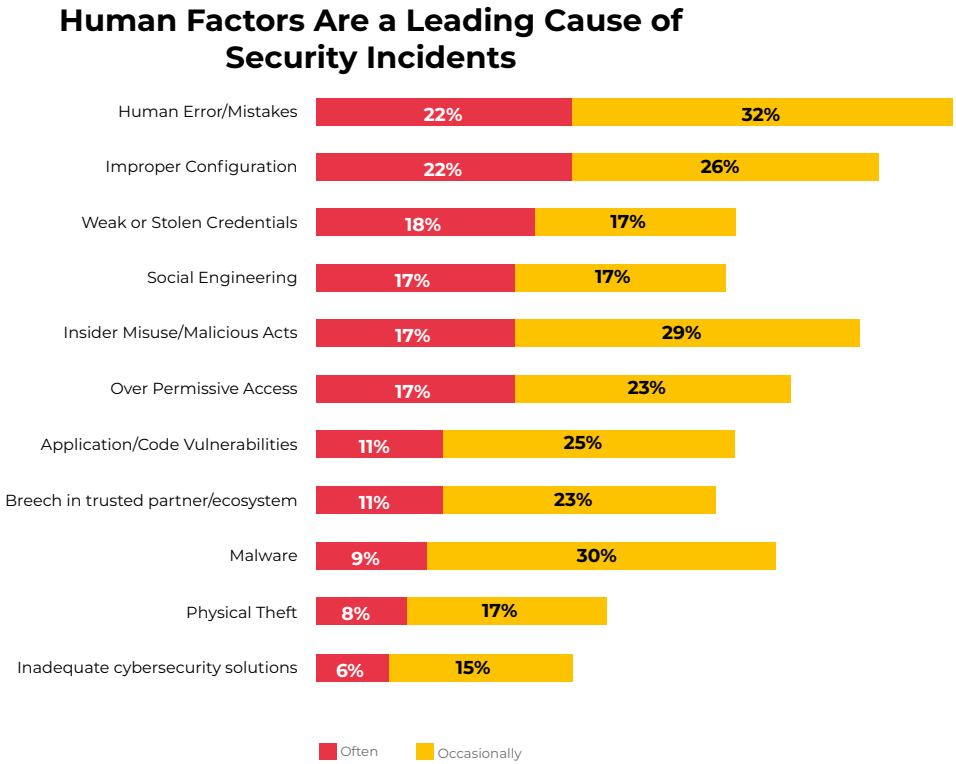

Figure 44: Human factors and configuration issues outpace malware as the most common causes of security incidents.

Top-Reported Causes of IT Security Incidents

Respondents assessed how frequently various causes contributed to incidents in their organization. Based on the combined share of "Often" and "Occasionally" responses:

- **53.9% cited "Human error or mistakes"** as a

frequent or occasional cause—making it the top vulnerability.

- **47.7% blamed "Improper configuration",** especially in cloud, network, and IAM settings.
- **46.1% pointed to "Insider misuse or malicious acts,"** confirming that internal risk is alive and well.
- **40.0% reported "Over-permissive access controls" as a contributing factor.**
- **39.1% identified malware infections** as an ongoing concern—though lower than human-centric issues.

At the lower end of the spectrum, physical theft, software supply chain risks, and third-party exposure were mentioned less frequently—but not insignificantly.

Interpreting the Root Cause Trends

- **Security is Only as Strong as Your Users and Configs** The leading causes are not advanced attacks—they're operational and procedural oversights.
- **Insiders Remain a Quiet Threat** Whether accidental or deliberate, employee actions account for a large share of breaches—especially with access to sensitive systems.
- **Malware Takes a Back Seat to Missteps** Traditional malware isn't gone—but its prominence is slightly lower compared to process failures and privilege mismanagement.

> 64% of enterprises are retraining their technical staff to meet evolving threats—AI, cloud, and IAM skills are in highest demand.

CIO Action Agenda

- Build a culture of secure operations—combine training with real-time feedback and consequence modeling.
- Implement configuration management and continuous validation tools—especially across cloud and SaaS environments.
- Audit and restrict access based on least privilege principles—review regularly and automate provisioning wherever possible.
- Strengthen insider risk programs that combine user behavior analytics (UBA) with education and deterrence.

Key Insight

The biggest threats may not be external—they're often already inside the firewall. To reduce incident frequency, enterprises must focus as much on **process and people** as they do on **perimeter protection.**

Takeaways for Ecosystem Partners

- **Vendors** should provide configuration drift detection, IAM hygiene tools, and contextual UBA platforms.
- **Consultants** can add value by mapping operational risk, access exposure, and internal control weaknesses.
- **Training providers** must evolve offerings to go beyond awareness—into behavior change, simulation, and accountability.

Bottom Line

Cybersecurity starts with discipline, not just defense. By addressing the mundane but material causes—misconfiguration, over-access, and human error—CIOs can reduce incident volumes dramatically without waiting for the next major tool or zero-day.

CLOUD SECURITY AND GOVERNANCE IS COMPLICATED

As enterprises deepen their cloud adoption, their security posture is increasingly tested by dynamic environments, decentralized ownership, and composable architectures. The 2025 SoT survey confirms that the biggest cloud security challenges stem not from the cloud itself—but from how it's configured, integrated, and governed.

Cloud security is now less about perimeter defense—and more about internal clarity and control.

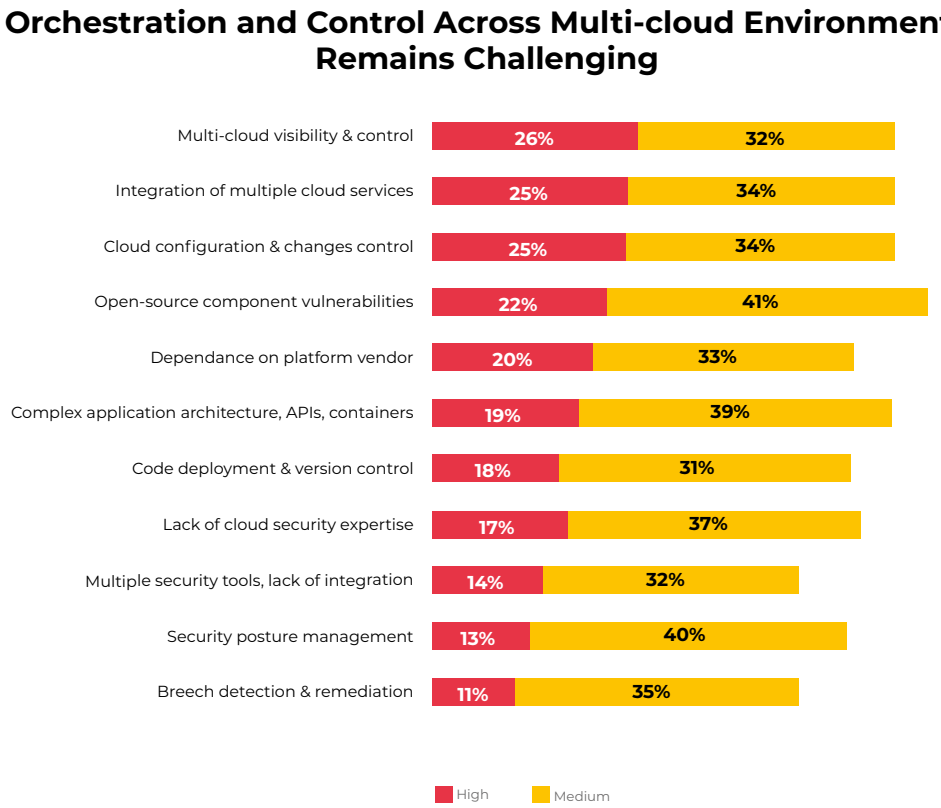

Figure 45: Visibility, integration, and open-source risks top the list of cloud security pain points.

What Do Enterprises Struggle With Most in Cloud Security?

Based on the share of respondents rating each challenge as high or medium in severity, here are the top areas of concern:

- **62.5% cited "Open-source component vulnerabilities"** as a significant challenge—underscoring growing reliance on unvetted libraries and dependencies.
- **58.5% flagged both "Cloud configuration & change control" and "Integration of multiple cloud services."**
- **58.5% also expressed concern over "Multi-cloud visibility & control."**
- **57.8% pointed to "Complex application architectures" involving APIs, containers, and microservices.**

Other issues such as compliance mapping, identity access sprawl, and CSP-native tooling gaps also surfaced, but with lower intensity.

What This Reveals About the State of Cloud Security

- **Component Risk Is Underestimated** Many enterprises don't actively inventory or validate the security posture of third-party components—leaving gaps in the supply chain.
- **Configuration and Change Control Are Core Weaknesses** Misconfigurations—often in IAM, storage, or networking—are a top source of exposure in cloud environments.
- **Multi-Cloud Means Multi-Blindspots** As cloud estates grow, so do the challenges of policy consistency, observability, and access governance.
- **Architecture Is Outpacing Security Design** DevOps, containerization, and microservices bring agility—but can outstrip the reach of traditional security tooling.

CIO Action Agenda

- Deploy automated tools for cloud security posture management (CSPM) and open-source software scanning.
- Implement least-privilege access and enforce tagging, versioning, and logging policies across environments.
- Build centralized cloud governance frameworks—even in federated or multi-cloud setups.
- Align SecOps and DevOps to integrate security earlier in the development and deployment pipeline (shift left).

Key Insight

The cloud isn't inherently insecure—but its dynamic, distributed nature creates complexity. Enterprises must secure not just workloads, but also the glue—the configurations, APIs, and components that connect everything.

Takeaways for Ecosystem Partners

- **CSPs and security vendors** must offer better native tooling and integrations—especially for hybrid and multi-cloud use cases.
- **Integrators and consultants** can help enterprises design and enforce secure cloud architecture blueprints.
- **Open-source communities and sponsors** must prioritize CVE transparency, lifecycle support, and security patching.

Bottom Line

The cloud has changed how we build and run applications—but not how attackers think. To protect in the cloud, CIOs must enforce visibility, automate hygiene, and simplify governance—because complexity is the new vulnerability.

SECURITY PRACTICES ARE MATURING UNEVENLY

In an era of hybrid work, zero trust, and cloud-first operations, identity and access management (IAM) is more central than ever. The 2025 SoT survey shows that while Indian enterprises have made strong progress in deploying authentication tools like MFA and SSO, foundational practices like identity governance and role-based access control (RBAC) still trail in implementation maturity.

IAM readiness is uneven—anchored in control, but still maturing in strategy.

Maturity of IT Security Processes is Extensive across Policy and Operation Parameters

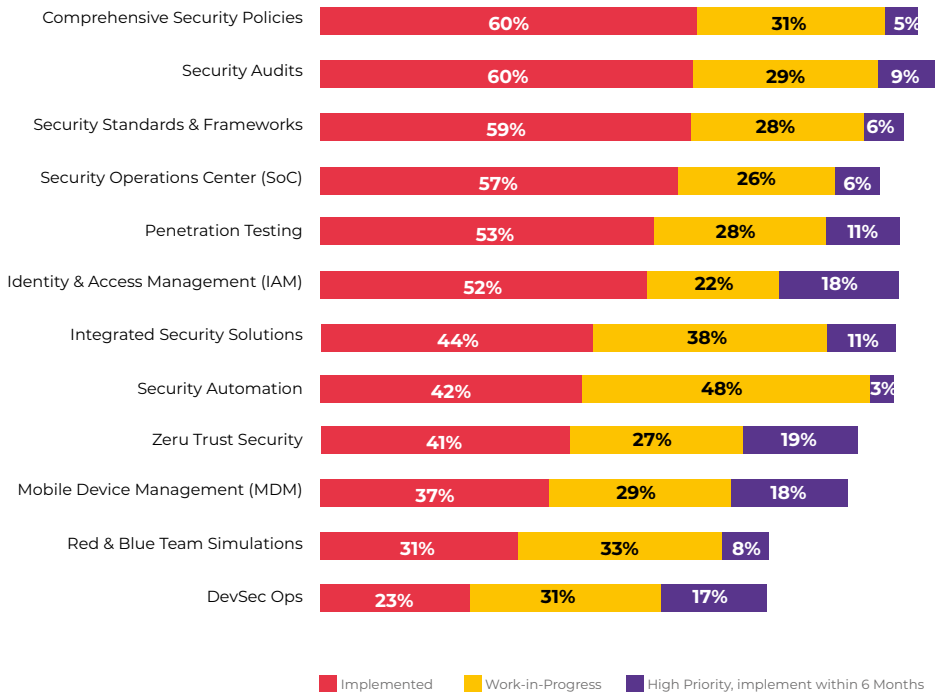

Figure 46: Core controls like audits and policies are widely implemented—advanced practices like simulations, automation, and DevSecOps still ramping up.

Which Security Processes Are Well Established—and Which Are Catching Up?

Based on combined rates of full implementation and work-in-progress deployment, the most mature practices are:

- **Comprehensive security policies (90.8%)—**the most broadly adopted foundational control.
- **Security automation (89.2%)—**reflecting growing comfort with SOAR and scripting.
- **Security audits (89.2%) and Security standards/ frameworks (87.5%)** also show strong adoption.
- **Security Operations Centers (SoCs) (83.1%)** are relatively well embedded, though still evolving.

At the other end of the spectrum:

- **DevSecOps has only 23.1% implementation,** with another 30.8% in progress.
- **Red/blue team simulations** show slightly higher implementation at 31.3%, but still limited penetration.
- **Mobile device management (MDM) and Threat intelligence platforms are** also lagging in full implementation.

Reading the Maturity Map

- **Controls Are in Place—Now Comes Coordination** Policies, frameworks, and audits show that enterprises have invested in documentation and basic governance.
- **Security Automation is on the Rise** Many have moved beyond manual operations, using orchestration tools to improve detection, triage, and response.
- **Proactive Defense is Still Emerging** Practices like red teaming, threat hunting, and purple teaming remain niche—often due to cost, complexity, or skill gaps.
- **Mobile and DevSecOps Are the New Frontiers** With remote work and CI/CD pipelines growing, these areas represent the next big leap in maturity.

CIO Action Agenda

- Maintain core governance momentum—refine policies and audits for dynamic environments.
- Expand automation from infrastructure to identity and incident response.
- Invest in simulation and red-teaming exercises—especially as threat sophistication grows.
- Treat DevSecOps as a capability—not a tool—by embedding security into software development lifecycle.

Key Insight

Most enterprises have secured the basics—but are still catching up to the pace of modern development, mobility, and threat complexity. Security maturity is not about having a checklist—it's about integration, automation, and proactivity.

Takeaways for Ecosystem Partners

- **Security vendors** should bundle red-teaming, MDM, and DevSecOps modules into platform offerings—not as optional add-ons.
- **Consultants** can support DevSecOps implementation roadmaps and maturity benchmarking.
- **Training providers** should focus on hands-on simulation, threat modeling, and CI/CD security integration.

Bottom Line

Foundational security is in place—but future readiness demands integration with how apps are built, how users work, and how threats evolve. CIOs must move from control to capability—from static compliance to dynamic defense.

SECURITY MANAGEMENT: CLOUD-DELIVERED, PARTNER-SUPPORTED, INTERNALLY ANCHORED

How enterprises manage their cybersecurity operations today reflects the broader shifts in IT—towards hybrid infrastructure, distributed teams, and platform-centric delivery. The 2025 SoT survey confirms that Indian organizations are embracing flexible models that combine internal control with external expertise, and on-premise deployment with cloud-based management.

Security management is no longer monolithic—it's modular, federated, and increasingly as-a-service.

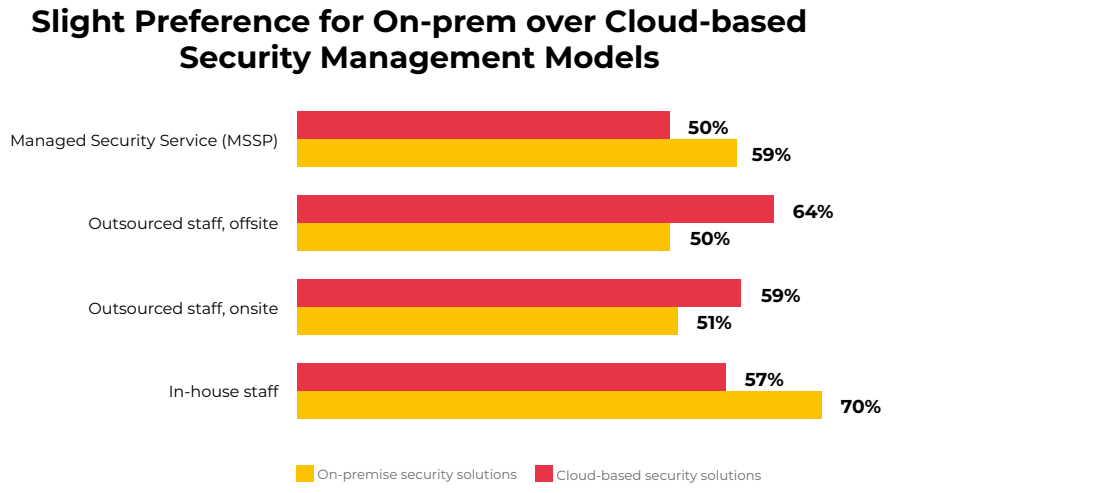

Figure 47: Most enterprises now blend cloud-managed tools with a mix of in-house, outsourced, and MSSP support.

How Security Is Being Deployed and Managed

Four main approaches dominate security management across enterprises, each showing a strong cloud shift:

- **In-house security teams remain foundational,** but more than half of these teams now use cloud-based tools to monitor and manage security operations.
- **Outsourced security staffing—both onsite and offsite—**is widely used, with the offsite model showing the highest cloud management preference.
- **Managed Security Services Providers (MSSPs)** are prevalent, especially for continuous monitoring and specialized services—though their use is more evenly split between on-prem and cloud-based delivery.
- Across the board, **cloud-based security management is on par or higher than on-**

premise approaches, indicating growing comfort with remote visibility, automation, and partner-led operations.

What This Signals About the Security Operating Model

- **Control Remains In-House, But Delivery Is Cloud-Based** Even when managed by internal teams, security functions are increasingly run from cloud consoles and integrated platforms.
- **Staffing is Distributed by Design** Many organizations are extending their teams with outsourced personnel—blending proximity with 24/7 coverage and specialist depth.
- **MSSPs Are Strategic Extensions, Not Replacements** Few enterprises outsource all security functions. Instead, they rely on MSSPs for scale, speed, and specific capabilities—especially in incident response, threat hunting, and compliance.

> About 77% of enterprises say phishing remains a top security threat despite years of training, GenAI-enabled deception continues to bypass human defenses.

CIO Action Agenda

- Define the optimal operating model for your organization—based on risk profile, resource maturity, and business complexity.
- Clarify governance and accountability across in-house staff, contractors, and MSSPs—especially during incident response.
- Use cloud-based tools and platforms to unify visibility, automate reporting, and streamline collaboration across models.
- Continually assess partner performance and in-house upskilling needs to maintain control and agility.

Key Insight

Security is no longer confined to one team or one platform. The new normal is a blend of internal oversight, external support, and cloud-powered operations—each reinforcing the other.

Takeaways for Ecosystem Partners

- **Tool vendors** must enable seamless collaboration between internal and external teams—through shared dashboards, RBAC, and open APIs.
- **MSSPs and service providers** should adapt to hybrid co-management models—where ownership and visibility are shared, not siloed.
- **Security integrators** can add value by helping clients operationalize platform-native tooling within distributed teams.

Bottom Line

Security leadership is no longer about doing everything in-house—it's about orchestrating everything effectively. The most secure organizations are those that combine people, partners, and platforms into a coherent, accountable, and responsive security function.

SECURITY CHALLENGES: THREAT VOLATILITY, TALENT SHORTAGES, AND REGULATORY COMPLEXITY LEAD

As organizations mature their security operations, the biggest roadblocks are shifting from tools to context. The 2025 SoT survey reveals that Indian enterprises now face challenges that span talent, regulation, and business alignment—alongside traditional concerns like threat complexity and budget constraints.

Security isn't just about defense—it's about dynamics: adapting to change across threats, teams, and laws.

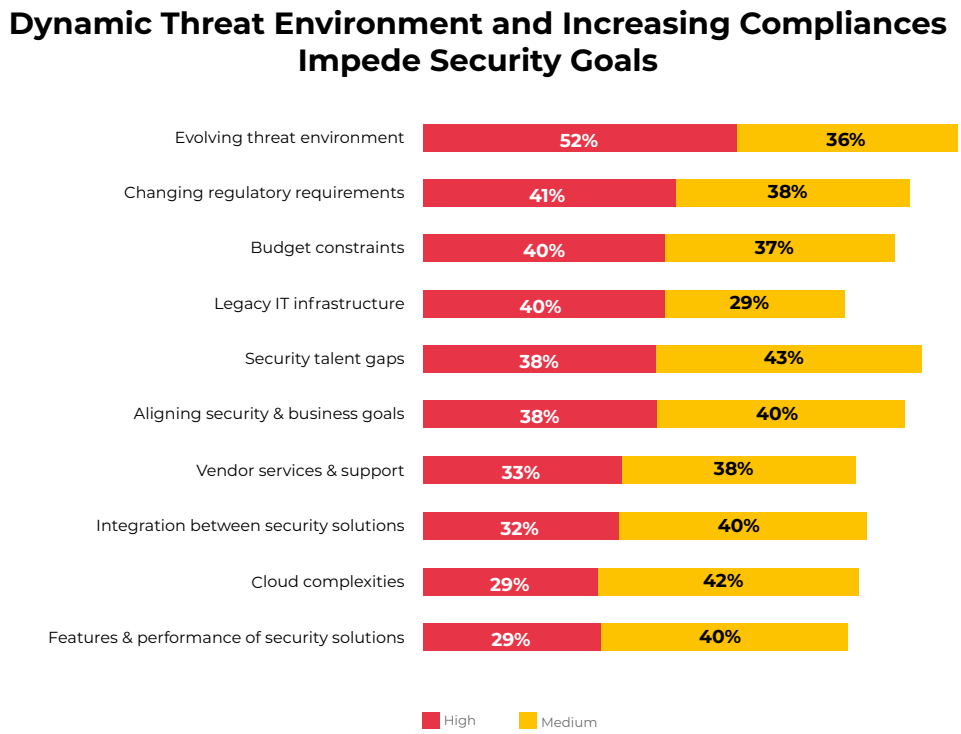

Figure 48: Enterprises cite evolving threats, hiring gaps, and compliance uncertainty as key barriers to cybersecurity success.

What's Getting in the Way of Security Goals?

Respondents ranked the challenges they face in achieving their IT security objectives. The most frequently cited issues, based on combined "High" and "Medium" impact, include:

- **87.5% cited the "Evolving threat environment"—**a reflection of how unpredictable and sophisticated attacks have become.
- **81.5% flagged "Security talent gaps",** with nearly 39% ranking it as a high-priority concern.
- **79.4% said "Changing regulatory requirements" are a significant barrier—**not surprising as privacy laws and data sovereignty mandates rise.
- **78.5% reported difficulty in "Aligning security with business goals."**
- **76.9% mentioned "Budget constraints,"** though slightly lower in perceived urgency than strategic or regulatory issues.

These findings show that even well-resourced security programs can struggle when internal alignment and external volatility aren't addressed.

What These Rankings Tell Us

- **Security Leaders Are Playing Catch-Up with Attackers** With threats evolving faster than defenses, proactive posture management and real-time response are under pressure.
- **People Gaps Undermine Progress** The lack of skilled cybersecurity professionals continues to hamper adoption of best practices, tool optimization, and strategic planning.
- **Compliance Is Becoming a Moving Target** From national data protection laws to global standards, enterprises must now manage overlapping—and often shifting—requirements.
- **Security Needs a Business Seat** Difficulty aligning with strategic priorities points to a persistent communication and governance gap between security and leadership teams.

CIO Action Agenda

- Invest in threat intelligence, continuous monitoring, and adaptive security to stay ahead of evolving adversaries.
- Prioritize upskilling, mentorship, and creative hiring to close security staffing gaps.
- Build compliance-by-design frameworks that map multiple regulations to operational workflows.
- Translate security metrics into business outcomes—resilience, reputation, and risk reduction—to secure greater buy-in and funding.

Key Insight

Security outcomes depend as much on clarity, capability, and collaboration as they do on controls. The roadblocks to maturity are systemic—not just technical.

Takeaways for Ecosystem Partners

- **Vendors** must simplify compliance mapping, cross-platform integrations, and threat intelligence consumption.
- **Service providers and MSSPs s**hould offer talent-augmented models to help enterprises bridge skill and strategy gaps.
- **Training partners** must go beyond certifications—focusing on real-world security thinking, automation, and cross-functional alignment.

Bottom Line

Security maturity is no longer about tools and technologies—it's a function of agility, alignment, and adaptability. CIOs who build resilient teams, stay ahead of regulation, and speak the language of the business will move faster and defend smarter.

IAM MATURITY: GOVERNANCE LAGS, MFA AND SSO LEAD

In an era of hybrid work, zero trust, and cloud-first operations, identity and access management (IAM) is more central than ever. The 2025 SoT survey shows that while Indian enterprises have made strong progress in deploying authentication tools like MFA and SSO, foundational practices like identity governance and role-based access control (RBAC) still trail in implementation maturity.

IAM readiness is uneven—anchored in control, but still maturing in strategy.

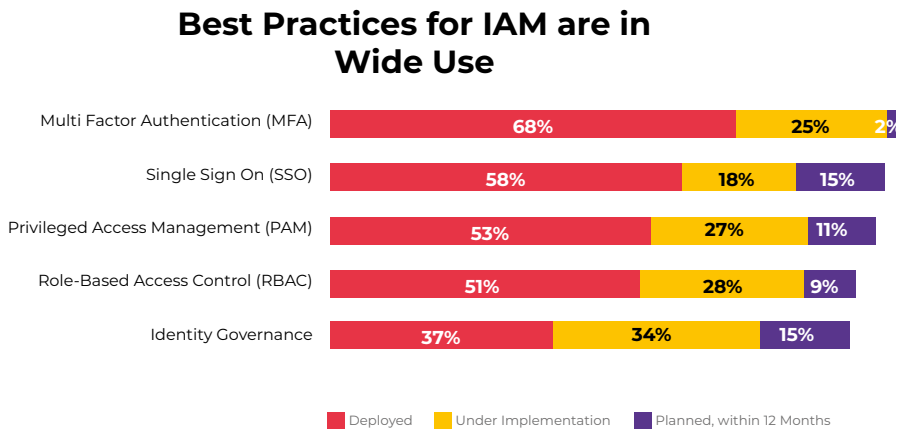

Figure 49: Authentication controls like MFA and SSO see strong adoption—identity governance and access modeling still evolving.

What IAM Capabilities Are in Place?

Respondents assessed their status across five key IAM components. The top trends based on combined "deployed" and "under implementation" rates are:

- **92.3% have Multi-Factor Authentication (MFA) either deployed or in progress,** with 67.7% reporting full deployment.
- **79.7% have deployed or are implementing Privileged Access Management (PAM)—** indicating strong concern about high-risk users.
- **78.5% show adoption of Role-Based Access Control (RBAC)—**critical for scalable, policy-driven access enforcement.
- **76.9% have deployed or are implementing Single Sign-On (SSO)** for consolidated identity experience.
- **70.8% are progressing with Identity Governance—**but only 36.9% have it fully deployed.

These results reflect a prioritization of perimeter and high-risk access controls over governance and lifecycle automation.

Interpreting the IAM Landscape

- **Authentication Comes First** MFA and SSO are now considered basic hygiene—especially

in regulated industries, or for remote access scenarios.

- **Privileged Access Is a Top Priority** With admin and elevated credentials under constant threat, PAM is no longer optional.
- **Governance Lags Behind** While some enterprises are advancing into automated provisioning, recertification, and compliance workflows, many still manage identity lifecycle manually or ad hoc.
- **RBAC Is Important—but Not Easy** Designing effective roles and enforcing them across systems requires both cultural buy-in and tool integration.

> Nearly 54% of organizations report business disruption as the biggest cyber fallout, showing that attacks now hit where it hurts most: operations and uptime.

CIO Action Agenda

- Enforce MFA and SSO universally—including for SaaS apps, third parties, and developers.
- Expand PAM coverage beyond admin accounts to service accounts, cloud consoles, and DevOps pipelines.
- Build a business case for identity governance automation—linking it to audit, compliance, and provisioning efficiency.
- Invest in RBAC design workshops and cross-functional access review processes to support scalable enforcement.

Key Insight

Enterprises have embraced the tools of IAM—but the programs around governance, provisioning, and role modeling still need to mature. Authentication is the starting point—not the finish line.

Takeaways for Ecosystem Partners

- **IAM vendors** should provide modular platforms that allow enterprises to start with controls (e.g., MFA) and grow into governance.
- **System integrators** can support end-to-end IAM rollouts—from architecture to policy design to access lifecycle automation.
- **Consulting partners** must help link IAM to broader business goals—compliance, risk reduction, and digital workforce enablement.

Bottom Line

Identity is the thread that connects users, devices, data, and cloud. CIOs who treat IAM as a strategic capability—not just a compliance checkbox—will gain control, agility, and user trust.

DATA PRIVACY: ASSESSMENTS AND CONSENT LEAD, ANONYMIZATION LAGS

With rising regulatory scrutiny and customer expectations around data protection, enterprises are embedding privacy into their digital and data initiatives. The 2025 SoT survey reveals that while most organizations have made progress in privacy impact assessments (PIAs) and consent management, deeper operationalization—like automating data subject rights or anonymizing data—is still evolving.

Privacy programs are shifting from policy to practice—but not yet to full maturity.

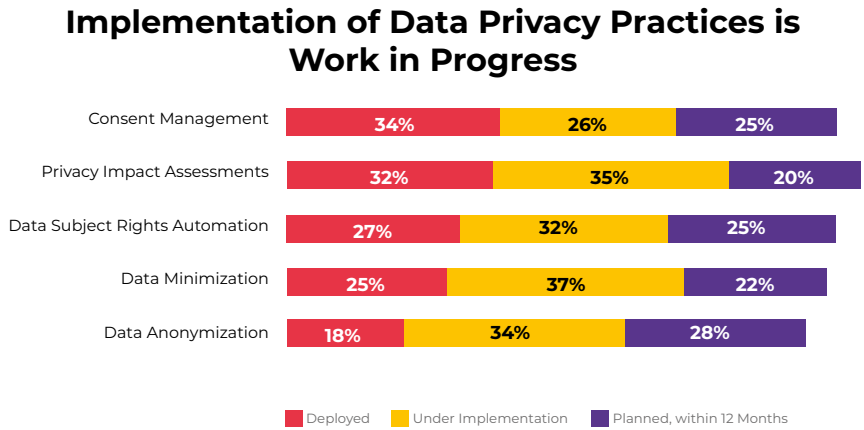

Figure 50: Most enterprises are implementing PIAs and consent mechanisms—data minimization and rights automation still maturing.

Where Enterprises Stand on Privacy Practices

Respondents rated their implementation status across five key privacy-enabling practices. Based on combined "Deployed" and "Under Implementation" shares, the leading practices are:

- **Privacy Impact Assessments (PIAs): 67.7% active adoption,** with over 32% fully deployed.
- **Data Minimization: 61.5% combined adoption,** a foundational principle that ensures only necessary data is collected and retained.
- **Consent Management: 60.0% active,** reflecting growing need for granular, revocable, and documented user permissions.
- **Data Subject Rights Automation (e.g., access, correction, deletion): 58.7%,** with a large share in progress.
- **Data Anonymization: only 52.3% actively adopted,** and 20% of enterprises have no current plans to implement it.

These results reflect a prioritization of perimeter and high-risk access controls over governance and lifecycle automation.

Interpreting the Privacy Practice Landscape

- **Assessments and Consent Are Leading the Charge** Most enterprises have responded to data protection laws by prioritizing risk assessments and user consent workflows.
- **Minimization is a Principle—But Not Yet a Practice** While widely acknowledged, actual controls to enforce data minimization during collection or processing are still catching up.
- **Rights Automation Is a Work in Progress** Many enterprises are manually handling data subject access and deletion requests, limiting scalability and audit-readiness.
- **Anonymization Is Often Overlooked or Understood** Despite its role in reducing risk and enabling data reuse, anonymization is complex to implement—and rarely prioritized unless mandated.

> Close to 63% highlight open-source vulnerabilities as a leading cloud risk, reflecting how third-party components have become the soft underbelly of enterprise security.

CIO Action Agenda

- Institutionalize PIAs across new systems, vendors, and process changes—not just during major IT projects.
- Integrate consent management into customer and employee-facing apps—linking it to real-time permissions management.
- Operationalize data minimization by aligning with application design, data architecture, and retention policies.
- Build workflows and automation around rights requests to reduce manual handling and legal exposure.
- Educate teams on anonymization methods—and integrate into analytics and data sharing initiatives.

Key Insight

Enterprises are taking privacy seriously—but often at a superficial level. Moving from checklists to embedded practices will require tighter integration between IT, legal, data teams, and customer experience leaders.

Takeaways for Ecosystem Partners

- **Privacy platforms and SaaS vendors** must offer modular tools that support PIAs, consent logging, data lineage, and rights automation.
- **System integrators** can bridge compliance goals with IT delivery—embedding privacy into workflows, APIs, and logs.
- **Policy advisors and trainers** should help organizations interpret evolving regulations into concrete, repeatable actions.

Bottom Line

Privacy is no longer optional—but it is not just a legal issue. It's a design, process, and data architecture issue. CIOs who embed privacy into the core—not bolt it on—will earn trust, and stay ahead of compliance curves.

CLOSING THE SECURITY SKILLS GAP WITH RE-TRAINING AND PARTNERING

With cybersecurity demands growing faster than talent pipelines, Indian enterprises are adopting a multi-pronged approach to bridge the gap. The 2025 SoT survey shows that most organizations are focused on retraining existing staff, engaging with external experts, and simplifying security operations to reduce the skill burden.

It's no longer just about hiring—it's about enabling.

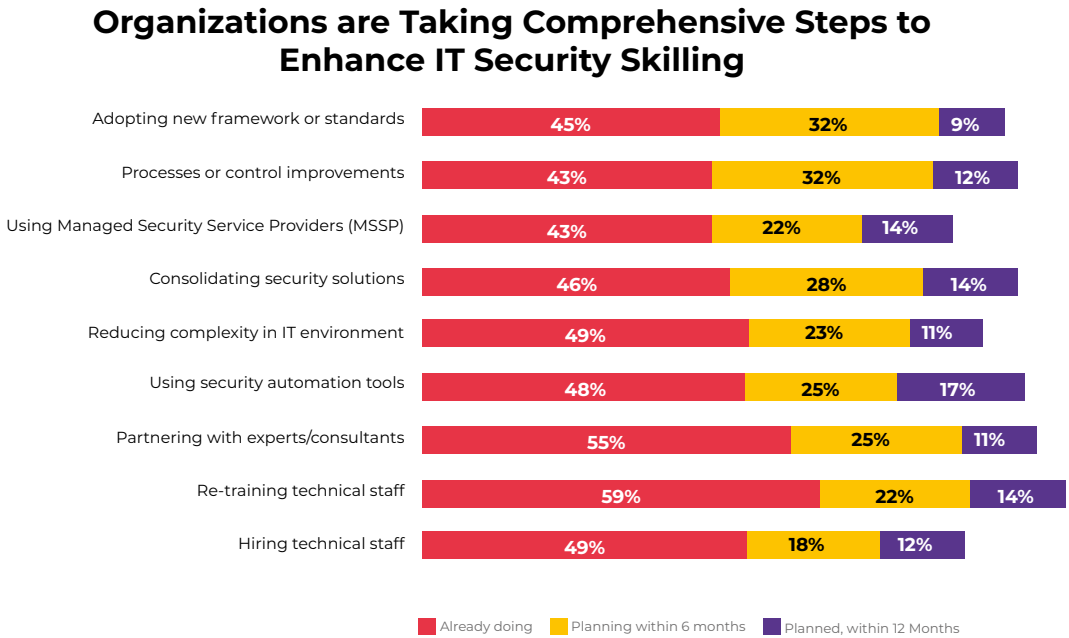

Figure 51: Enterprises favor internal upskilling and strategic partnerships over headcount expansion alone.

What Are Enterprises Doing to Address the Skills Challenge?

Respondents indicated what actions they are currently taking or planning in the next 6 – 12 months. Based on the share of organizations already implementing these actions:

- **59.4% are retraining technical staff,** making it the most widely adopted strategy.
- **55.4% are partnering with external experts or consultants** to gain immediate expertise.
- **49.2% are hiring new technical staff—**a significant investment, but not the primary lever.
- **49.2% are simplifying their IT environments,** a smart move to reduce operational complexity and skill dependency.

- **47.7% are turning to security automation tools** to reduce manual workloads and improve scalability.

Together, these responses paint a picture of enterprises looking to rebalance their talent strategies—less reliant on raw hiring, more focused on enablement and efficiency.

What the Strategies Reveal

- **Upskilling Is the First Line of Defense** With the pace of change outstripping hiring pipelines, organizations are focusing inward—training existing talent to take on more specialized roles.
- **External Expertise Fills Urgent Gaps** Consultants and partners provide just-in-time coverage, especially for specialized roles like threat hunting, IAM design, or audit prep.
- **Simplification Is a Strategic Enabler** Rationalizing platforms, standardizing policies, and consolidating tools reduce both cognitive and administrative load on security teams.
- **Automation Bridges Talent and Time** With lean teams, automation helps scale detection, response, and reporting—without compromising security posture.

> Over 83% expect AI to impact incident response within 18 months—automated triage and remediation are fast becoming standard SOC capabilities.

CIO Action Agenda

- Make reskilling a strategic program—invest in modular, role-specific training tied to business priorities.
- Leverage partnerships to access specialized skills and accelerate delivery—especially in cloud, IAM, and compliance.
- Audit the IT and security stack for complexity—rationalize, retire, and consolidate wherever possible.
- Expand security automation from alerts to orchestration—reducing manual dependencies in routine operations.

Key Insight

Solving the skills gap isn't just about supply—it's about strategy. The most mature enterprises are enabling talent through training, simplifying their operations, and complementing internal teams with trusted partners.

Takeaways for Ecosystem Partners

- **Training providers** should deliver outcome-driven, stack-specific security curricula that go beyond certifications.
- **Consultants and MSSPs** must offer flexible engagement models—filling gaps without displacing internal ownership.
- **Tool vendors** should emphasize usability, integration, and out-of-the-box automation to minimize complexity.

Bottom Line

The security skills gap won't vanish—but it can be mitigated. Enterprises that reframe the problem as a design, enablement, and collaboration issue will build stronger, more resilient teams—without being caught in a perpetual hiring race.

AI'S SECURITY IMPACT: DETECTION AND RESPONSE LEAD THE WAY

Artificial intelligence is no longer a distant promise in cybersecurity—it's becoming an embedded reality. The 2025 SoT survey reveals that Indian enterprises expect the greatest near-term impact of AI in operational areas like incident response, threat detection, and network management. These functions demand speed, pattern recognition, and continuous improvement—natural fits for AI augmentation.

Security teams aren't replacing analysts with AI—they're amplifying their reach, visibility, and reaction time.

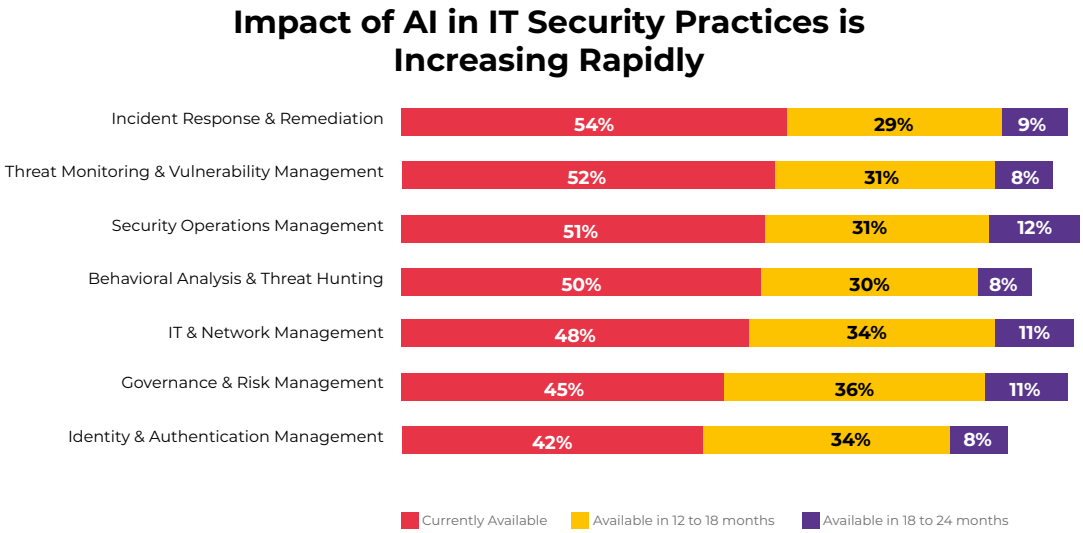

Figure 52: Enterprises expect AI to significantly influence incident response, monitoring, and operations within 18 months.

Where AI Will Quickly Make A Difference

Respondents were asked when they expect AI to materially impact various security functions. Based on those who cited current availability or impact within 12–18 months, these areas lead:

- **Incident Response & Remediation (83.1%)—**the highest near-term impact, driven by use of AI for alert triage and playbook automation.
- **IT & Network Management (82.3%)—**AI is increasingly used for anomaly detection, baseline modeling, and traffic analysis.
- **Threat Monitoring & Vulnerability Management (82.3%)—**another area seeing early AI adoption for prioritization and correlation.
- **Security Operations Management (81.5%)—**AI helps with log analysis, case management, and behavioral analytics.

- **Governance & Risk Management (81.3%)—** emerging applications include AI-assisted risk scoring, policy validation, and reporting.

In every category, over 80% of respondents expect AI to make an impact within 18 months—indicating broad readiness and relevance.

Decoding the AI Security Timeline

- **Detection and Response Are First to Automate** These functions are data-heavy and time-sensitive—making them ideal for machine learning, pattern recognition, and predictive analytics.
- **AI in Governance and Identity Is Rising—but More Gradually** Risk management and access control use cases are still emerging—often requiring higher maturity and data quality.
- **Adoption Is Broad, Not Niche** With nearly all core security functions expected to benefit from AI in the near term, the conversation is now about scale—not skepticism.

> Nearly 88% of organizations say threat volatility is their biggest cybersecurity hurdle—keeping pace with attackers is now a full-time strategy.

CIO Action Agenda

- Prioritize AI in detection and response workflows—starting with alert enrichment, prioritization, and automated remediation.
- Ensure AI security tools integrate with SIEM, SOAR, and threat intelligence feeds for maximum visibility.
- Pilot AI applications in risk and governance—focusing on accuracy, transparency, and compliance alignment.
- Upskill security teams to work alongside AI—focusing on analysis, oversight, and escalation rather than repetitive triage.

Key Insight

AI is becoming embedded in the modern SOC—not as a replacement for human judgment, but as a force multiplier. The biggest benefits lie in automation, prioritization, and response agility.

Takeaways for Ecosystem Partners

- **Vendors** must offer explainable, integration-ready AI features—especially for detection, correlation, and case management.
- **Consultants** can help enterprises assess where AI fits in the security lifecycle—and how to build trust in its outputs.
- **Training providers** should prepare analysts to interpret and supervise AI decisions—not just operate traditional tooling.

Bottom Line

AI is already shaping security's future—it's just not evenly distributed. Enterprises that invest in applied AI today will gain faster insights, leaner operations, and sharper defenses tomorrow.

AI ANXIETY: PHISHING, DEEPFAKES, AND DATA LEAKAGE

AI is fast becoming an indispensable part of modern cybersecurity—but its adoption also raises serious concerns. The 2025 SoT survey shows that Indian security leaders are most worried about AI being turned against them—whether through deepfakes, phishing, or model manipulation. Risks from over-reliance, third-party AI tools, and opaque decision-making further add to the caution.

The consensus: AI's benefits are real—but so are its dangers.

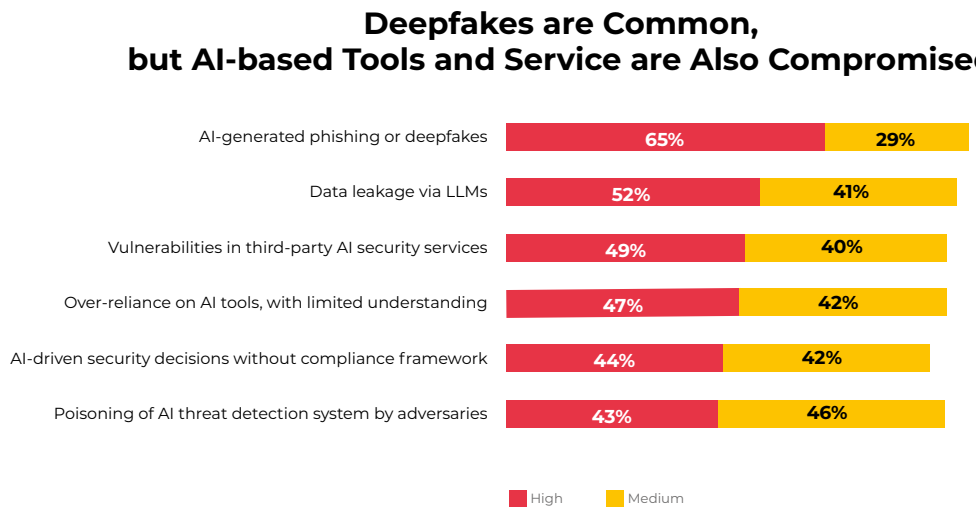

Figure 53: With 93.9% of respondents marking it as high or medium risk, AI-generated deception tops the threat list.

Top Concerns About AI Use in Cybersecurity

Respondents ranked potential risks associated with integrating AI into security operations. Based on the combined share of "High" and "Medium" concern, these emerged as the top five:

- **AI-generated phishing and deepfakes (93.9%)—**by far the most cited concern, reflecting how adversaries use GenAI for deception and impersonation.
- **Data leakage via LLMs and AI platforms (92.2%)—**particularly relevant as teams experiment with chatbots, assistants, and cloud-based tooling.
- **Poisoning of AI threat detection models (89.2%)—**highlighting fears of adversarial inputs compromising accuracy.
- **Vulnerabilities in third-party AI security services (89.2%)—**underscoring risks introduced by toolchains, APIs, or unmanaged models.
- **Over-reliance on AI without human understanding (89.1%)—**pointing to concerns about automation without interpretability or override mechanisms.

These concerns reflect a blend of **external threats** (e.g., manipulation, deception) and **internal risks** (e.g., blind trust, lack of transparency).

What the Concerns Tell Us

- **Offensive AI Is Here** Tools like deepfake generators and GenAI-enhanced phishing kits are already in use—forcing defenders to adapt quickly.
- **Data Exposure Is a Two-Way Street** The same AI tools used to analyze security logs can inadvertently leak sensitive data if improperly configured or trained.
- **Trust Without Transparency Is Dangerous** "Black-box" AI decisions, especially in detection or response, create audit, bias, and accountability risks.
- **Third-Party AI Tools Bring New Attack Surfaces** AI modules embedded in broader platforms or MSSP workflows may not be fully vetted—leading to unknown vulnerabilities.

> Around 71% have initiated identity governance, but just 37% have fully implemented it—revealing a gap between access control intent and execution.

CIO Action Agenda

- Strengthen phishing and impersonation defenses with media forensics, zero-trust communications, and user education.
- Apply strong access controls and data masking when using AI tools—especially LLMs with external APIs or cloud access.
- Validate AI model inputs and outputs—monitor for poisoning attempts or performance drift.
- Keep a human-in-the-loop for AI-assisted decisions, particularly in remediation and policy enforcement.

Key Insight

The rise of AI in cybersecurity brings a dual-edged challenge: protecting with AI—and protecting against AI. Security teams must embrace innovation while building guardrails to contain its misuse.

Takeaways for Ecosystem Partners

- **AI security vendors** must provide explainability, audit logs, and adversarial resilience—not just faster detections.
- **Tooling platforms** should offer sandboxed environments for AI models and limit sensitive data exposure during inference.
- **Governance and risk advisors** can help enterprises craft responsible AI adoption policies with cybersecurity at the core.

Bottom Line

AI is a powerful ally—but also a high-stakes experiment. CIOs who move fast without guardrails risk amplifying vulnerabilities. The winners will be those who integrate AI thoughtfully—balancing speed with scrutiny, and automation with accountability.

Key Contributors

Giridhar has more than 35 years of experience in areas spanning media, consulting and digital technology, working with leading B2B and B2C media organizations across the Asia-Pacific region. He has been actively involved with professional communities in developing content-driven engagements and platforms, and people recognition programs.

R. Giridhar
Group Editor
9.9 Group

Deepak is an analyst, columnist, and speaker with more than 35 years of experience in various market research, advisory, and editorial roles spanning domains such as IT, telecom, and sustainability. His focus areas include market and trend analysis, strategic communications, and internal and external sales enablement.

Deepak Kumar
Founder Analyst & Chief Research Officer
BM Nxt

With over 18 years of experience in research, consulting, media, and communication, Jatinder Singh currently serves as the Executive Editor at CIO&Leader. He is responsible for shaping the editorial strategy and direction of the publication. He specializes in writing about cutting-edge topics such as analytics, artificial intelligence, cloud computing, the Metaverse, and cybersecurity.

Jatinder Singh
Executive Editor - CIO&Leader
9.9 Group

CIO&LEADER

CIO&Leader is India's leading platform for enterprise technology leaders and decision-makers. It serves as a catalyst for the exchange of well-informed perspectives and insights, and fosters discussions on cutting-edge trends, technology implementations and use cases, IT business strategies, leadership, and innovation between CIOs and other key stakeholders.