IDC PERSPECTIVE

Key Software Delivery Challenges and Pain Points in 2026: AI Further Snarls Existing Complexity of Cloud-Native Landscape

George Mironescu

EXECUTIVE SNAPSHOT

Owing largely to the nondeterministic nature of large language models (LLMs), AI and agentic AI derivatives substantially amplify software delivery complexity. Engineering leaders must address technical debt, fragmented environments, skills gaps, and regulatory demands, while AI's nondeterministic nature heightens risk and delivery pressure. Success requires thinking and execution that balance pragmatic and strategic considerations.

Key takeaways

- With AI dominating the delivery agenda and strong pressure from senior leadership to productize it, delivery risks are significantly rising.
- AI inflates the complexity of software delivery, compounding existing technical and nontechnical engineering challenges.
- Beyond AI architectural and integration complications, the most severe delivery pain points include upskilling for cloud native, bridging legacy and modern environments, and embedding security into pipelines, all while ensuring compliance.
- To succeed, organizations must treat AI as a strategic priority, yet approach transformation in a phased, measured manner, where adoption gets scaled in line with proven value realization.

Recommended actions

- Establish robust governance frameworks for AI adoption, ensuring compliance with regulatory requirements and internal policies, and implement phased, board-level oversight to manage risk exposure and value realization.
- Modernize application and data infrastructure to cloud-native architectures, prioritizing Kubernetes-native environments and aligning data, cloud, and AI road maps and engineering agendas.

February 2026, IDC #US54277526

- Integrate security across the entire AI-data-application delivery life cycle, including by enhancing security expertise within data and AI engineering teams.
- Manage vendor relationships with a strategic view on platform and environment readiness, midterm dependencies, and demonstrable ROI.

SITUATION OVERVIEW

Software delivery has always been inherently difficult. The operating environment is vectorized by intertwined issues and pressure points including technical debt, legacy platforms, intermittent modernization, prolonged mandates to improve release cadence and quality, environment fragmentation, tooling sprawl, and persistent skills gaps.

But with the arrival of AI, complexity levels are spiraling owing to the nondeterministic nature of outputs and behavior of AI systems, the underlying engineering complexity imposed by new software and hardware components, and the emergence of new knowledge domains (e.g., LLM engineering, GPU-AI-app workload optimization).

Triangulating complexity: AI, cloud native, and security

IDC survey data shows that engineering leaders expect elevated difficulty across virtually every major delivery consideration in the next 12 months (see Figure 1). Yet **complexity of AI architectures and AI integrations, upskilling for cloud-native and AI practices, managing the gap between legacy and cloud-native environments,** and **integrating security into delivery pipelines** emerge as the most severe challenges they expect to face in 2026. Beyond these challenges, **meeting regulatory requirements is nonnegotiable** for virtually every organization, therefore paramount for any software engineering endeavor undertaken.

FIGURE 1

Challenges for software engineering/delivery organization in the next 12 months

Q. How challenging will each of the following be for your software engineering/delivery organization in the next 12 months?

n = 1,048

Source: IDC's *Worldwide AI and Cloud-Native Software Delivery Survey*, November 2025–January 2026

Relative to monolithic software architectures, AI, cloud native, and the security landscape compound complexity across every phase of the software development life cycle and every layer of the stack. They act as challenge multipliers due to their novelty, risk profile, and latitude and depth through which they create architectural and organizational dependencies:

- AI is reshaping how software is built and delivered, but at the very same time it cascades complexity at every level of the stack, from silicon to the data layer. Engineering leaders are under pressure to integrate AI rapidly, often without mature governance models or standardized delivery patterns.
- Operating AI inference at a reasonable cost entails robust cloud-native industrialization and acquisition of new skills, from container orchestration to distributed observability.

- Furthermore, security risks are spiraling on the back of AI with vulnerability and compliance concerns capable of halting progress entirely. This forces orgs to make security more integral to software delivery — the case for DevSecOps becomes more compelling than ever.

AI implementations face complex web of obstacles

A broad distribution of significant and critical challenges underscore that AI adoption is not constrained by a small set of dominant issues. Instead, organizations are facing a wide landscape of technical, organizational, and business constraints (see Figure 2).

On the technical side, the most severe challenges, especially for platform teams, relate to ensuring AI activities remain always compliant with legal requirements and internal governance policies. Grappling with aging software delivery platforms is also a big pain point for platform teams as they need to integrate AI pipelines with legacy workflows and practices.

Data availability and readiness continue to limit engagement with AI models down the value stream. Also, model life-cycle management, including observability of model behavior and model performance optimization, presents major operational challenges across the AI data engineering value chain.

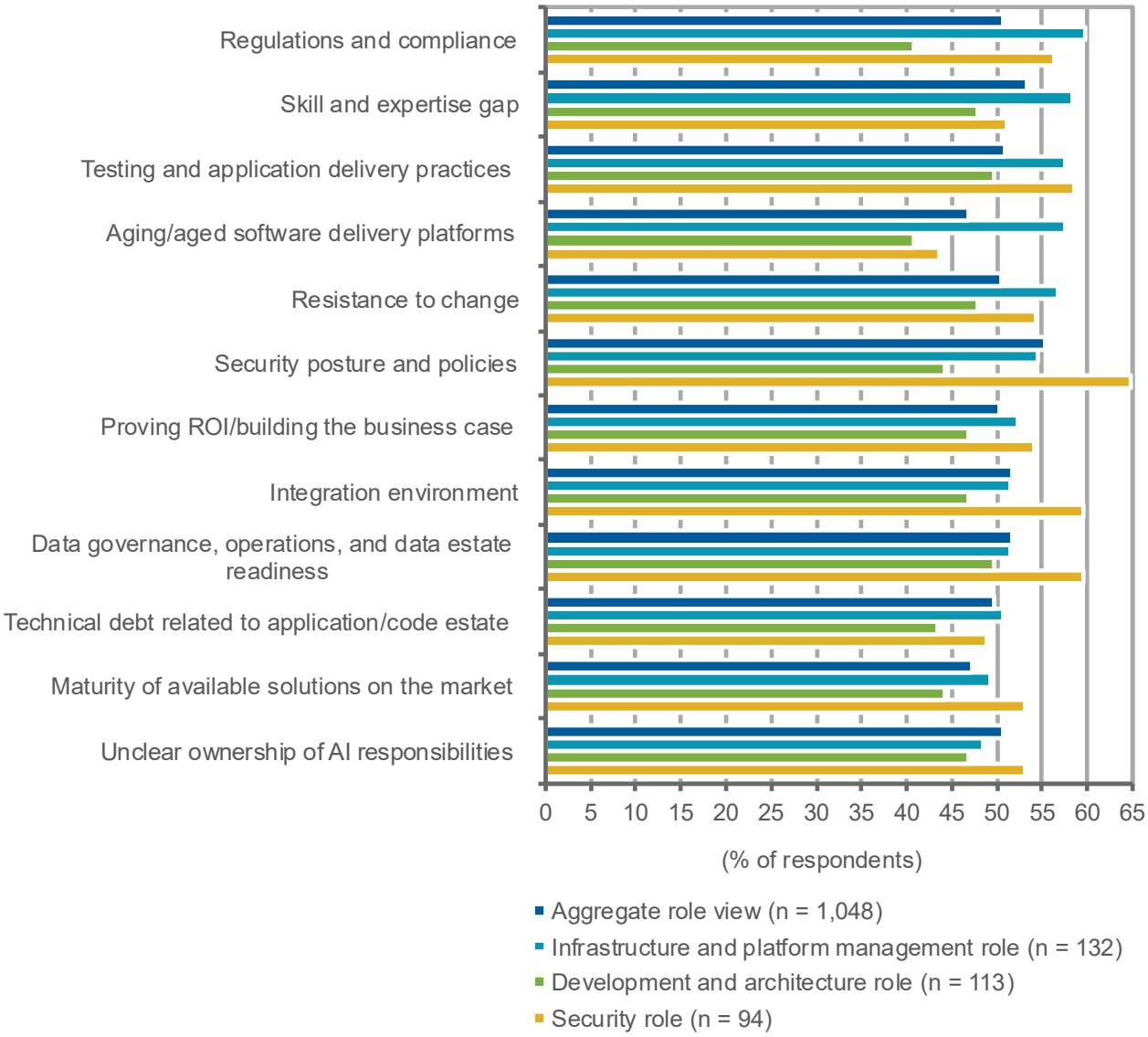
Firming up the security posture is particularly critical with the CISO and their security operations teams. 36% of security leaders indicate that security is a critical challenge to enabling AI within the application estate, followed by another 39% that identify it as a significant challenge.

Nontechnical challenges are equally material. Skills and expertise gaps, inertia and change management friction, and internal alignment between IT, security, and business stakeholders further compound implementation complexity. Current application estates were not designed for autonomous AI capabilities, and this is challenging existing testing and delivery practices. Furthermore, many organizations continue to struggle with establishing risk management capabilities and putting policies in place to ensure control, regulatory compliance, accountability, and decision rights in AI and AI agent-driven workflows.

FIGURE 2

Key AI/agentic AI implementation challenges

Q. How much of a challenge are the following factors when implementing AI or agentic AI within your application estate?



Source: IDC's *Worldwide AI and Cloud-Native Software Delivery Survey,* November 2025–January 2026

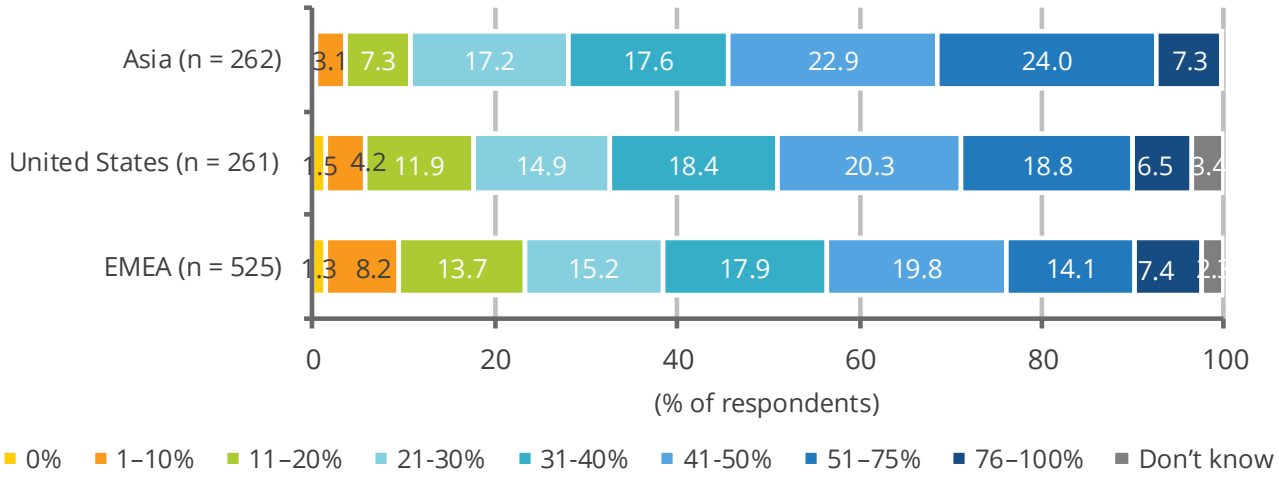
AI overwhelms agenda amid diverse priorities

Nearly half of organizations now report that a significant portion of their IT initiatives are dominated by AI-related efforts, underscoring how deeply AI has penetrated the software delivery agenda (see Figure 3).

FIGURE 3

Software delivery initiatives related to implementing AI within the application estate by region

Q. Of the software delivery initiatives your organization scheduled for 2025, what share is related to implementing AI capabilities within your application estate?



Note: Asia coverage included China, India, and South Korea.

Source: IDC's *Worldwide AI and Cloud-Native Software Delivery Survey,* November 2025–January 2026

This change was particularly evident in the composition of project portfolios in 2025. A substantial proportion of organizations (i.e., 45%) indicate that more than 40% of their software delivery efforts were directly related to infusing AI in their application estates.

This clearly points out that for almost half of the software engineering organizations, AI is setting the priority, not competing for priority. Compared with other technology deployment initiatives, AI now commands disproportionate leadership attention.

As a result, software delivery organizations are being reshaped around AI-first requirements where software engineering teams need to adapt expertise and processes to effectively transition from experimentation to actual product delivery — this reflects pressing business expectations from senior management levels for AI-enabled outcomes.

High pressure to productize AI increases delivery risk

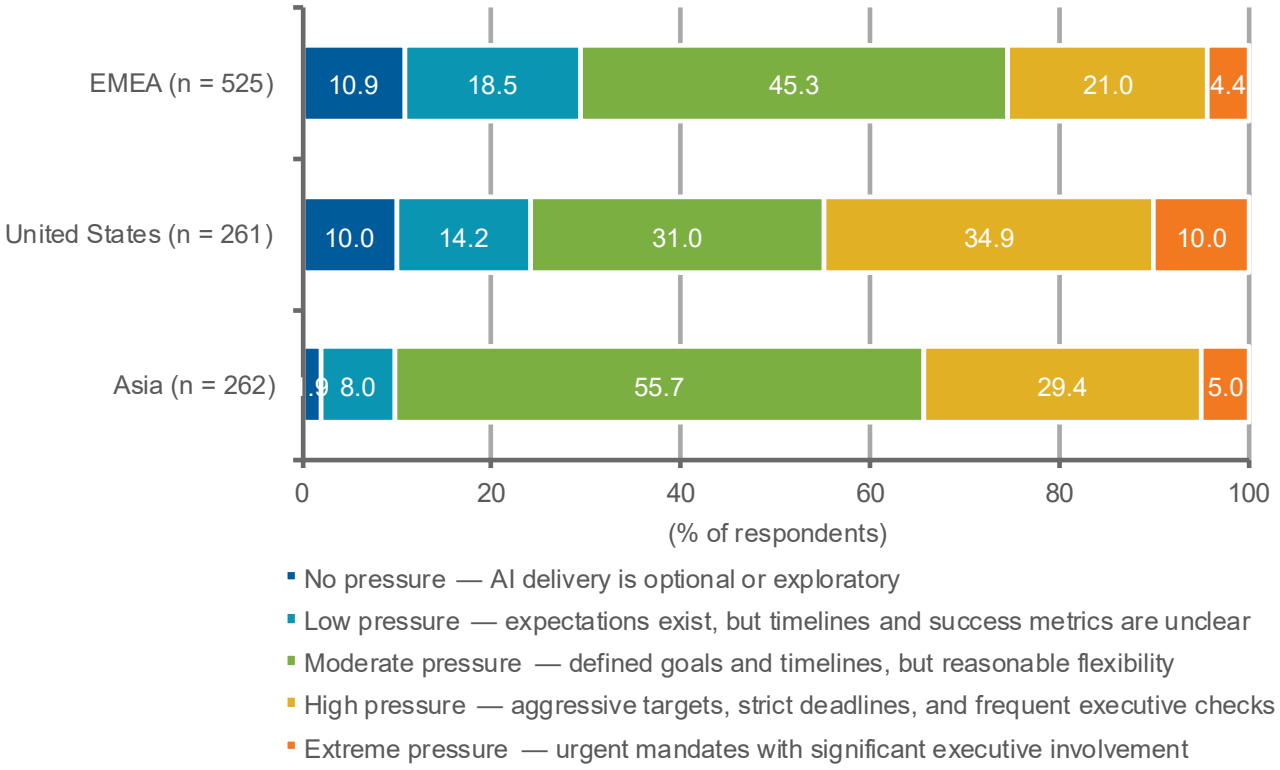
Pressure to turn AI ambition into tangible value is very evident, especially in specific geographies and with specific software delivery teams. Roughly one-third of software engineering leaders face **high or extremely high pressure** from senior leadership to

deliver AI applications. This pressure underscores how central AI has become to enterprise strategy (see Figure 4).

FIGURE 4

Software delivery organizations under strong pressure to make AI applications a reality by region

Q. What level of pressure is senior leadership placing on the software delivery organization to make AI applications a reality?



Source: IDC's *Worldwide AI and Cloud-Native Software Delivery Survey,* November 2025–January 2026

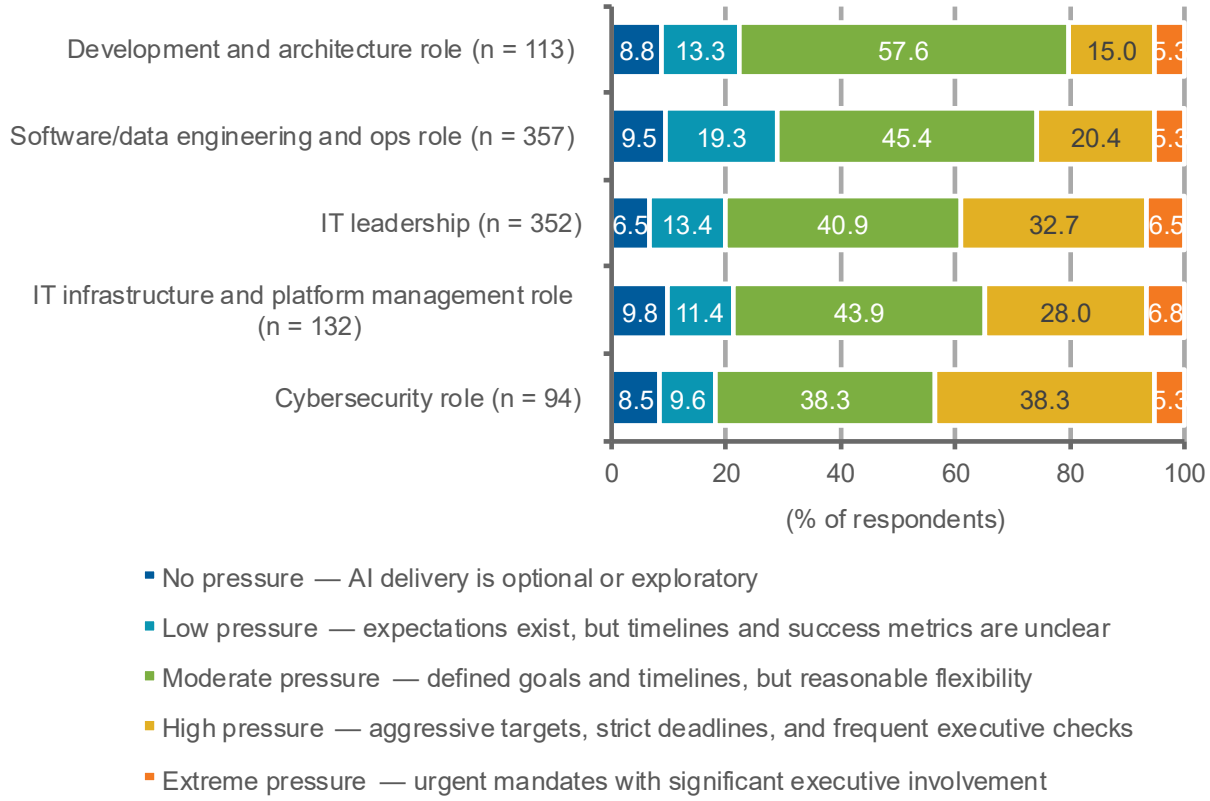
The pressure is particularly high in the United States where one in every ten software delivery organizations is under extreme pressure to deliver on AI ambitions. For these organizations, urgency in execution and close senior leadership supervision indicate that AI implementations are no longer treated as exploratory projects and that there are pressing mandates to show investment returns.

This level of pressure increases delivery risk, particularly where data and architectural readiness, governance, skills availability, or platform maturity fall short of requirements (see Figure 5).

FIGURE 5

Software delivery organizations under strong pressure to make AI applications a reality by delivery role

Q. What level of pressure is senior leadership placing on the software delivery organization to make AI applications a reality?



Source: IDC's *Worldwide AI and Cloud-Native Software Delivery Survey,* November 2025–January 2026

The closer a role is to enterprise risk, the higher the pressure

Pressure is uneven by role and intensifies as risk increases. Cybersecurity feels the most acute pressure, as seen also from the severity of challenges they cite in relation to AI implementations. Security has historically been stigmatized by dev teams as a bottleneck, and the pressure comes from the placement in value creation chain, especially in more traditional software delivery organizations where security is often located at the end of the pipeline. IT leadership is second in terms of pressure acuteness, as it carries final accountability for product delivery and demonstrated value.

Closing reflections: Choosing both pragmatism and vision

While many engineering leaders will be tempted to address software delivery in 2026 by optimizing at the margins, the winning organizations in the midterm will be the ones that rethink their delivery based on the triangulation between **AI engineering, cloud-native engineering,** and **security/governance and compliance realignment.** Organizations that continue to manage these areas via insular approaches are likely to experience friction and limited returns even in the short term.

At the height of the digital transformation hype cycle, delivery excellence was about working faster within existing constraints. Throwing more tools and more checkpoints at a problem was a typical way to move forward. Senior engineering leadership was largely assessed through the quality of the developer experience they enabled. In at-scale scenarios, AI is ballooning complexity orders of magnitude more. This is forcing organizations to reconsider their system of delivery to be able to ensure output is deterministic, explainable and compliant; and have grip on technical debt.

Organizations that treat AI as an additive technology layer may be gaining short-term benefits, but such strategy is likely to increase medium- to long-term complexity, technical debt, and cost.

The midterm enterprise race in AI demands both pragmatism and vision, where AI is treated as a strategic goal and not a mere tactical capability. With that in view, the AI frontier compels the IT leadership to enforce platforms standardization where applicable, cloud-native stack modernization, pervasive policy-as-code management, and life cycle–integrated security — as key technical prerequisites to scalable AI.

Note: All numbers in this document may not be exact due to rounding.

ADVICE FOR THE TECHNOLOGY BUYER

The wide range of critical and significant challenges in software delivery and AI implementations indicates that teams may lack direction regarding what to prioritize and where to start from.

Beyond the specific business goals and enterprise maturity of every organization, adapting the governance with a view on the risks and benefits AI is introducing, modernizing data and application architectures and practices to cloud native, and weaving security into the core of AI-data-application life cycle are important aspects to consider when shaping the IT strategy and sourcing/vendor engagement.

Clearly define the scope and limits for AI adoption

AI adoption should be approached as a controlled, incremental evolution of the enterprise technology landscape, guided by engineering discipline and board-level oversight. For engineering teams, this requires introducing AI within a clearly bounded application and organizational context while adapting governance and risk controls to that defined scope. Any governance adaptations must be anchored in compliance with existing regulatory obligations and internal policies.

From the board level, this phased approach should provide transparency into risk exposure, regulatory alignment, and value realization, ensuring that AI initiatives align to the organization's risk appetite and operating obligations. Validating architectural integrity, data governance, security controls, and operational accountability for a controlled environment should be key procedural steps when defining the foundation for AI adoption.

Modernize application and data infrastructure to cloud native

AI enablement is dependent on how well organizations reengineer their application and data infrastructure. Modernizing application and data delivery for Kubernetes-native environments is a prerequisite to effectively and efficiently manage AI from experimentation to system-level scaling and day 2 operations. Having a selective modernization approach in specific parts of the organization reduces risk, provides less costly learnings for higher-scale systems/environments, and reduces team/operational disruption and likely friction.

At organizational design level, it is important to ensure that data, cloud, and AI road maps are aligned and responsible teams are intimately understanding each other's goals and engineering roles.

Make security integral to AI-data-application delivery life cycle

The "shift left" mantra and the emergence of DevSecOps that drove much of the application delivery philosophy of the past 5–10 years needs to be reconsidered beyond the application perimeter and into the data and AI/agentic AI model development. Security capabilities need to permeate data science and data engineering, both via expertise acquisition among data and AI model engineering teams but also via closer involvement of security into the data and model life cycle. From policy definition and regulatory alignment to audits and transparency reports, to drift monitoring, SBOMs and supply chains oversight, placing security at the heart of every model engagement is key to lower AI operational risks.

Final considerations: Manage vendor relationships with eye on strategic dependencies

Almost half of engineering leaders note that maturity of available solutions on the market is low. This needs to be understood in the context of a still rapidly evolving technical

landscape and limited presence of industry standards and protocols. Furthermore, this consideration needs to be coupled with the fact that half of these leaders also point to limited cases of proven ROI and sound business case.

Entering vendor arrangements should happen with a clear eye on likely midterm dependencies these engagements create. At a strategic level, readying the platform and application landscape for AI should be a guiding consideration. At a tactical level, proving value and demonstrating investment return should guide vendor engagement.

LEARN MORE

Related research

- *IDC FutureScape: Worldwide Developer and DevOps 2026 Predictions* (IDC #US53858525, October 2025)
- *From Cloud-Native to AI-Native Software Engineering: How Strategic Considerations Are Shifting* (IDC #EUR153764425, September 2025)
- *Market Analysis Perspective: Worldwide Cloud-Native Software Engineering, 2025* (IDC #US52864325, September 2025)

Synopsis

This IDC Perspective looks into the challenges and pain points in 2026 for software delivery, which faces escalating complexity as AI integration compounds existing cloud-native and security challenges. Organizations must navigate technical debt, legacy systems, skills gaps, and regulatory demands while rapidly productizing AI under intense leadership pressure.

“Success hinges on pragmatic modernization of data and application infrastructure, embedding security throughout the life cycle, and clear-eyed vendor engagement,” said George Mironescu, associate research director, Software Development, Software Delivery, Software Engineering at IDC.

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global headquarters

One Beacon Street
Suite 33100
Boston, MA 02108
USA
508.872.8200
X: @IDC
blogs.idc.com
www.idc.com