theCUBE research

southworks

Enterprise Cloud Maturity and Strategic Gaps

Paul Nashawaty
Principal Analyst | theCUBE Research

December 2025

Executive Summary

With infrastructure, security, and application delivery increasingly centered around hybrid and multi-cloud strategies, the modern enterprise is essentially a cloud-driven entity. Based on an extensive survey of cloud architects, cloud decision makers, and cloud-native Azure professionals, we identify a high level of cloud maturity, especially within the Microsoft Azure ecosystem, as well as critical strategic gaps across the four main pillars of Cloud Infrastructure and Governance: Data & Security, Applications, DevOps & AI/ML Ops, and Agentic AI.

Key findings reveal that among our respondent base, predominantly enterprise IT decision-makers and cloud architects working in hybrid environments, Azure adoption reached 93.4%, reflecting the Microsoft-centric ecosystems these practitioners operate within. These organizations face complicated multi-cloud management challenges and a hefty security mandate, with security cited as the top cloud migration challenge by 53.5% of respondents. While organizations are heavily investing in AI/ML (74.3% actively train models), a major risk is exposed by the reliance on public AI tools (50.7%), which threatens data governance and enterprise security.

This study provides strategic insights to coordinate, safeguard, and expedite digital transformation initiatives by framing these pervasive enterprise trends into an actionable Gap/Solution framework.

Unifying Cloud Infrastructure and Governance

Hybrid cloud is the cornerstone of today's enterprise technology stack, with a pronounced preference for Azure adoption and increasingly complex multi-cloud operating models. While this reflects a high degree of cloud maturity, it also introduces a critical challenge: enforcing consistent automation and governance across heterogeneous environments without slowing delivery.

Current State of the Cloud Foundation

Azure-Centric Respondent Base: The survey captured organizations deeply embedded in Azure environments, with 93.4% of respondents reporting an Azure presence. This sample composition reflects the Microsoft-centric cloud strategies prevalent among the enterprise IT decision-makers and cloud architects surveyed, providing valuable context for understanding their infrastructure priorities, governance challenges, and modernization approaches.

Resilience is a Priority: Operational resilience is well established. A majority of respondents (60.7%) deploy workloads using multi-region active/passive architectures, while 46.8% physically separate production and non-production environments and 46% enforce logical separation. These practices indicate strong operational discipline and a clear prioritization of stability and security.

Multi-Cloud Account Sprawl: Despite this maturity, complexity continues to rise. Nearly two-thirds of organizations (61.3%) operate between 6 and 20 cloud accounts or projects across AWS, Azure, and GCP. This level of sprawl increases the difficulty of maintaining consistent security policies, cost controls, and compliance postures without centralized automation.

Strategic Gap: Infrastructure-as-Code Fragmentation

Strategic Gap	Data Point Evidence from Survey Data	Impact on Operations
Multi-cloud drift and inconsistent Infrastructure-as-Code	CloudFormation adoption at 76%; Terraform at 55.5%; Azure DevOps used by 82.9% for CI/CD	Platform-specific IaC leads to configuration drift, duplicated effort, and inconsistent governance across environments

Strategic Response: SOUTHWORKS Unified Platform Engineering

To address IaC fragmentation and multi-cloud drift, SOUTHWORKS applies a unified, cloud-agnostic platform engineering model built around standardized, declarative Infrastructure-as-Code.

Rather than maintaining parallel automation stacks, organizations consolidate on a common IaC framework that spans Azure, AWS, and GCP. This approach reduces configuration drift, enforces policy-as-code consistently, and simplifies auditability across environments.

By aligning Azure DevOps pipelines with standardized IaC practices, SOUTHWORKS enables enterprises to preserve their existing tool investments while achieving greater consistency and control. This is an increasingly critical capability as hybrid and multi-cloud environments become the norm.

The PII Imperative and Migration at Scale in Data and Security

Data is essential to cloud computing, and its security cannot be compromised, especially in regulated sectors. According to our research, the great majority of organizations handle sensitive data and are dealing with heavy migration workloads. Therefore, having strong secrets management and modern security tools is essential.

Current State of Data and Risk

PII is Ubiquitous: An overwhelming 90.8% of organizations store and process Personally Identifiable Information (PII). Combined with the fact that 78.3% are subject to industry regulations such as HIPAA or GDPR, data privacy and compliance are no longer edge cases; they are foundational operational requirements.

Cloud-Native Data Storage: Data platforms continue to migrate toward managed cloud services. More than half of respondents (55.5%) rely on managed cloud databases, while an additional 33.8% use SaaS-based database services. This shift reduces operational burden but places increased emphasis on network security, identity controls, and application-layer protections, particularly for the remaining 10.7% still operating self-hosted databases.

Migration Workloads are Substantial: Cloud migration is ongoing and substantial. Nearly half of respondents (44.5%) are migrating 25–50% of their data, while 40.8% are migrating 50–75%. At the same time, tolerance for downtime is extremely low: 49.7% of organizations consider only 1–6 hours of downtime acceptable for traffic cutover. This combination creates intense pressure to execute migrations with both speed and precision.

Security Tooling and Secrets Management Maturity: Security tooling is specialized and widely adopted, with Aqua (66.8%), Wiz (47.7%), and Snyk (42.8%) leading usage. Furthermore, 66.5% of organizations store secrets in Azure Key Vault, indicating strong alignment with cloud-native best practices for credential and secrets management.

Strategic Gap: Security as the Primary Migration Constraint

Strategic Gap	Evidence from Survey Data	Impact on Operations
Security and compliance slow cloud data migration	53.5% cite security as the top migration challenge; 40.8% migrating 50–75% of data	Data integrity, PII protection, and compliance validation become bottlenecks, increasing risk and delaying cutover

Contrary to earlier phases of cloud adoption, it is security, not cost or tooling, that is now the dominant constraint on migration velocity. As enterprises move increasingly large volumes of sensitive data, the risk of data exposure, integrity loss, or regulatory non-compliance grows exponentially.

Traditional security models treat compliance validation as a late-stage checkpoint, often occurring just before production cutover. In large-scale migrations with narrow downtime windows, this reactive approach introduces uncertainty, delays, and elevated operational risk. The result is a paradox: organizations invest heavily in security tools, yet security remains the primary blocker to progress.

Strategic Response: SOUTHWORKS Integrated SecOps for Secure Migration

To remove security as a migration bottleneck, SOUTHWORKS embeds security and compliance directly into the migration lifecycle rather than treating them as post-hoc validation steps.

Through integrated SecOps practices, automated data integrity checks, and continuous compliance validation, security becomes an active enabler of migration speed rather than a reactive gate. Compliance evidence is generated continuously, ensuring that data protection requirements are met before production cutover, not after.

By aligning cloud-native security tooling with automated validation workflows, SOUTHWORKS enables enterprises to migrate large-scale, regulated data sets with confidence and without sacrificing speed or compliance.

Accelerating Modernization in Applications, DevOps, and AI/ML Ops

Application modernization is characterized by hybrid architectures, with monoliths operating alongside microservices, and the overwhelming adoption of Python and Java. In addition to moving to the cloud, workloads are becoming increasingly accelerated and GPU-driven, with a strong emphasis on AI/ML.

Current State of Application Modernization

Hybrid Application Landscape: The modernization strategy is pragmatic. More than half of organizations (56.9%) are migrating both monoliths and microservices, confirming that lift-and-shift combined with targeted refactoring is the prevailing approach. This reflects a practical acknowledgment of the cost and complexity associated with full-scale microservices conversion.

Dominant Languages and Specialized Compute: Python (80.1%) and Java (76.3%) dominate application stacks, signaling continued investment in both data-intensive and AI-driven workflows (Python) as well as resilient enterprise back-end systems (Java). Supporting these workloads increasingly requires specialized infrastructure, with 76% of organizations already running GPU workloads—making high-performance, parallel processing a baseline requirement for modern applications.

AI/ML Operationalization at Scale: AI adoption is mature, with 74.3% of organizations actively training machine learning models. However, this maturity introduces a new operational challenge: 66.2% of existing ML pipelines require migration, creating demand for specialized MLOps tooling, infrastructure, and operational expertise.

Strategic Gap 1: Hybrid Migration Complexity

Strategic Gap	Evidence from Survey Data	Impact on Operations
Complexity of migrating monoliths and microservices simultaneously	56.9% migrating both monoliths and microservices	Without repeatable patterns, hybrid migration becomes costly, slow, and highly customized

Migrating both monolithic and microservices architectures requires a highly differentiated approach. While hybrid strategies reduce risk compared to full re-architecture, they also introduce operational complexity. Without clear patterns and repeatable processes, hybrid migrations often devolve into bespoke efforts that are difficult to scale, govern, or automate across teams and applications.

Strategic Response: SOUTHWORKS Monolith-to-Microservices Pattern

SOUTHWORKS applies a structured, phased modernization approach that incrementally refactors and decouples monolithic workloads into service-based architectures. This pattern minimizes risk by preserving critical dependencies while progressively introducing modularity.

By aligning refactoring efforts with deployment automation and operational best practices, this approach establishes a scalable foundation for continuous deployment and long-term application agility.

Strategic Gap 2: ML Pipeline Migration Overhead

Strategic Gap	Evidence from Survey Data	Impact on Operations
Complexity of migrating machine learning pipelines	74.3% actively train ML models; 66.2% of ML pipelines require migration	Poorly executed migrations disrupt training, deployment, and model lifecycle management

Migrating a traditional CI/CD pipeline is materially different from migrating a data-intensive, computationally demanding, and rapidly evolving machine learning pipeline. These pipelines underpin core AI capabilities, and disruption can directly impact model accuracy, deployment cadence, and business outcomes.

Without a structured approach, ML pipeline migration becomes a high-risk initiative that strains teams and threatens production stability.

Strategic Response: SOUTHWORKS MLOps Pipeline Migration Blueprint

SOUTHWORKS defines a repeatable blueprint for migrating and modernizing machine learning pipelines. By incorporating version control, automated validation, and modular orchestration, organizations reduce migration complexity while maintaining model accuracy and reproducibility.

This approach accelerates time to production and ensures that ML pipelines remain compliant, observable, and operationally resilient as they transition to modern cloud environments.

Strategic Gap 3: Monitoring and Operational Burden

Strategic Gap	Evidence from Survey Data	Impact on Operations
Monitoring and incident response burden on DevOps teams	44.5% monitoring led by DevOps; 38.7% shared responsibility	Operational overload diverts teams from innovation to reactive firefighting

Shifting monitoring responsibilities left to DevOps teams aligns with modern engineering practices, but it also introduces risk. As application and infrastructure complexity increase, monitoring and incident response can overwhelm internal teams, reducing their ability to focus on higher-value modernization and innovation initiatives.

Over time, this operational drag slows transformation efforts and increases burnout across engineering organizations.

Strategic Response: SOUTHWORKS Operational Agility Model

SOUTHWORKS addresses operational burden through a dual-tier model that combines Forward-Deployed Engineers (FDE) for proactive platform optimization with Sustained Engineering (SE) for ongoing maintenance and support.

This model allows organizations to maintain reliable, high-performing environments while freeing internal teams to focus on application modernization, AI initiatives, and business innovation, rather than constant firefighting.

Governance and Security in the Agentic AI Wild West

Agentic AI represents the evolution of enterprise computing, moving beyond traditional machine learning toward autonomous, goal-oriented systems. While adoption is accelerating rapidly, current implementations introduce significant governance and security challenges. These risks, particularly those involving sensitive and regulated data, require immediate attention.

Current State of Agentic AI Adoption

Reliance on Public AI Tools: More than half of organizations (50.7%) currently rely on public AI tools such as ChatGPT and Copilot. In contrast, only 20.2% report enterprise-wide deployments built on a common, governed framework. This fragmented, consumer-grade usage model strongly suggests limited control over proprietary data, prompts, and outputs.

Prioritized Capabilities Focus on Augmentation: Agentic AI adoption today is largely pragmatic and productivity-driven. Organizations prioritize:

- Automating repetitive tasks (73.1%)
- Decision optimization (71%)
- AI assistants (70.7%)
- Assisting workers in decision-making (67.5%)

This emphasis on augmentation over full autonomy indicates that while interest in advanced agentic systems is high, implementation remains focused on high-ROI, lower-risk use cases.

External Sourcing Dominates Adoption Strategy: To address skills gaps and accelerate adoption, organizations overwhelmingly rely on external expertise. Nearly three-quarters (70.9%) source agentic AI capabilities through platform vendors, while 68.6% engage IT or consulting service providers. Only 31.5% report building agentic AI capabilities primarily in-house.

Strategic Gap	Evidence from Survey Data	Impact on Operations
Monitoring and incident response burden on DevOps teams	44.5% monitoring led by DevOps; 38.7% shared responsibility	Operational overload diverts teams from innovation to reactive firefighting

The disparity between widespread public AI tool usage and limited enterprise-wide deployments represents a critical governance failure. In practice, this means that sensitive enterprise data (potentially including PII, regulated information, and proprietary intellectual property) is being passed to public large language models outside formal security and compliance controls.

This exposure is not hypothetical. As agentic AI becomes embedded in everyday workflows, uncontrolled prompt and data flows create a systemic risk that undermines data governance, regulatory compliance, and organizational trust. In regulated industries, this gap represents a material compliance violation waiting to surface.

Strategic Response: SOUTHWORKS Secure Enterprise AI Gateway

To mitigate data exposure risk while preserving productivity, SOUTHWORKS implements a centralized Secure Enterprise AI Gateway that governs all large language model interactions within enterprise boundaries.

This framework routes prompts, data, and responses through controlled environments where interactions are logged, monitored, and policy-enforced. By centralizing access and governance, organizations maintain the benefits of agentic AI while eliminating the risks associated with ungoverned public AI tool usage.

By combining centralized control with flexible access to large language models, SOUTHWORKS enables enterprises to adopt agentic AI responsibly by balancing innovation with the governance and security controls required at scale.

Conclusion: Strategic Imperatives for the Governed Cloud

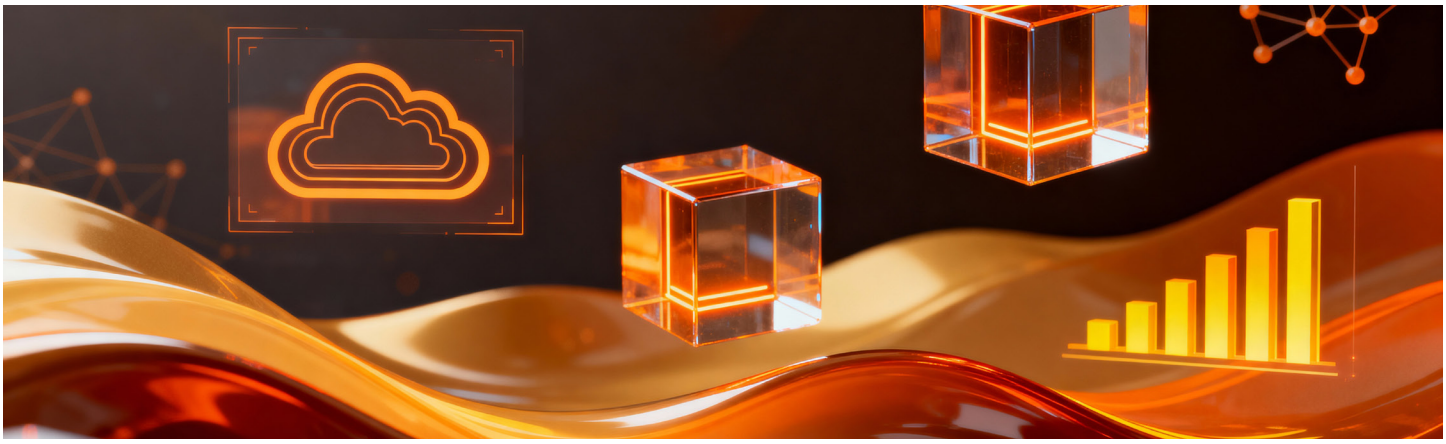
The enterprise cloud journey is at a critical juncture. While the high adoption rates of Azure (93.4%) and advanced technologies like GPU workloads (76%) demonstrate significant technical maturity, the strategic focus for the upcoming planning cycle must shift from adoption to unification and governance.

Our research reveals three critical fault lines that, if not addressed, will hinder future scalability and competitive differentiation:

1. Governance Deficit: The proliferation of platform-specific IaC (CloudFormation at 76%) alongside multi-cloud sprawl (6-20 accounts) creates inherent configuration drift and a costly governance deficit. Organizations are struggling to enforce policy-as-code consistency across heterogeneous environments.

2. Operational Drag: The burden of monitoring and incident response, largely pushed to DevOps (44.5%), introduces significant operational drag, diverting scarce engineering resources from high-value application modernization and ML pipeline migration (66.2% need migrating).

3. AI Security Erosion: The most immediate and critical security exposure is the reliance on un-governed, public AI tools (50.7%). This practice fundamentally compromises data security and regulatory compliance in an environment where PII is nearly universal (90.8%).



Analyst Take

Competitive advantage in the next era will be earned by those who prioritize controlled innovation instead of adopting cloud and AI technologies and governing them at scale. The solution lies in executing a focused strategic triad:

1. **Unified IaC** to centralize infrastructure control and eliminate configuration drift.
2. **Specialized Managed Services** to offload operational complexity and accelerate time-to-value for complex migrations, especially ML pipelines.
3. **A Secure Enterprise AI Gateway** to immediately close the critical data exposure vector from ungoverned public AI tool usage.

SOUTHWORKS aligns with these imperatives through a playbook approach that translates research findings into actionable frameworks. On the infrastructure and governance front, the company emphasizes standardizing Infrastructure-as-Code, consolidating tools such as Terraform across Azure, AWS, and GCP. This is especially relevant as most enterprises now manage between six and twenty cloud accounts. By unifying these practices, SOUTHWORKS enables measurable improvements in auditability, policy-as-code enforcement, and governance consistency—an area where few providers can successfully integrate Azure DevOps pipelines with Infrastructure-as-Code consolidation.

In operations and migration, SOUTHWORKS delivers managed services designed to relieve developer pain points. By reducing the operational drag of monitoring, observability, and incident response, the company allows teams to focus on innovation. Its repeatable patterns for monolith-to-microservices refactoring and MLOps migration blueprints, including containerization, feature stores, and Azure ML pipeline standardization, directly address the 66.2% of enterprises struggling with ML pipeline transitions. This combination of modernization acceleration and developer cycle efficiency is a key differentiator in the market.

AI security and governance are also central to SOUTHWORKS' approach. With 50.7% of enterprises still relying on public AI tools, the company's Secure Enterprise AI Gateway provides a timely safeguard. By routing all large language model traffic through a secure Azure environment, SOUTHWORKS allows organizations to maintain developer productivity while ensuring compliance, governance, and data protection. This positions the company as one of the few providers capable of combining AI-driven productivity with enterprise-grade security controls.

Disclaimer

All trademark names are the property of their respective companies. Information contained in this publication has been obtained by sources theCUBE Research, a SiliconANGLE Media company, considers to be reliable but is not warranted by theCUBE Research. The publication may contain opinions of theCUBE Research, which are subject to change. This publication is copyrighted by theCUBE Research, a SiliconANGLE Media company.

Contact

Silicon Valley
989 Commercial Street
Palo Alto, CA 94303

Boston Metro
95 Mount Royal Avenue
Marlborough, MA 01752

David Butler
david.butler@siliconangle.com
774-463-3400

theCUBE research