Hype Cycle for Operating Models, 2023

Published 25 July 2023 - ID G00791195 - 98 min read

By Analyst(s): Miguel Angel Borrega, Philip Dawson

Initiatives: I&O Organizational Strategy

An efficient operating model is crucial to improve IT governance, customer experience, employee engagement and productivity. I&O leaders should use this Hype Cycle to strategize and adopt operations patterns aligned with technologies to increase productivity while meeting their business needs.

Additional Perspectives

- ITオペレーティング・モデルのハイプ・サイクル：2023年
  (16 October 2023)

More on This Topic

This is part of an in-depth collection of research. See the collection:

- 2023 Hype Cycles: Deglobalization, AI at the Cusp and Operational Sustainability

Analysis

What You Need to Know

An operating model is a combination of organizational structures, processes, capabilities and relationships to conduct the daily activities of an organization to achieve the enterprise's strategic objectives.

A lack of an efficient IT operating model means the organization's strategy will not be executed properly, processes are not optimized and teams are misaligned to achieve business goals. This leads to inefficiencies and wasted effort that end in an IT organization not delivering business value. An IT operating model describes how and where critical IT operations should be done across a company.

The Hype Cycle

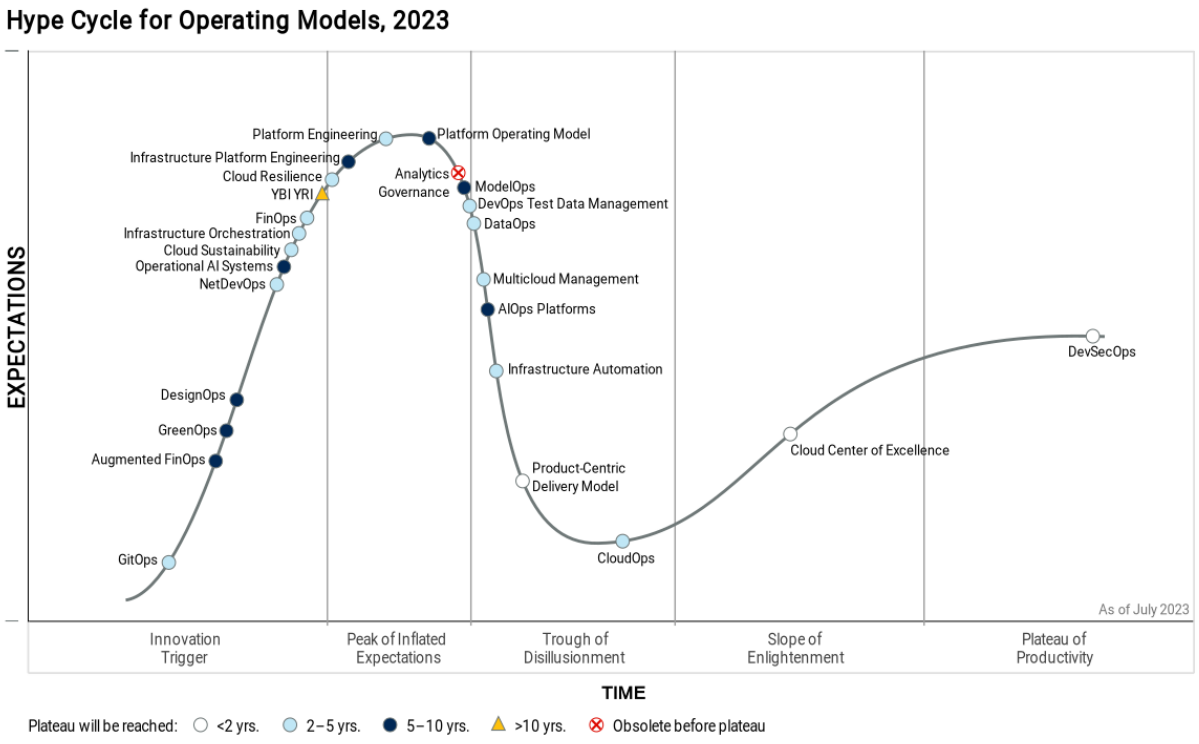
New and trending technologies are creating opportunities for business value. However, they often require evolving IT operations and procedures, governance models, team structures, and sourcing processes. Some examples:

- The way organizations consume cloud services (like infrastructure as a service [IaaS], platform as a service [PaaS] and SaaS) require different operation patterns, such as CloudOps and/or SaaSOps.
- Organizations move through different stages of maturity during their cloud adoption and need dedicated governance (e.g., cloud center of excellence) to be successful orchestrating multiple teams, management operations and sourcing.
- Shifting from one to multiple cloud providers requires implementing more complex management processes and operations, or adopting new cloud management tools, or delegating these management activities to external managed services providers.
- The application of artificial intelligence/machine learning and data analytics to current business data and processes is demanding operational AI systems and analytical governance.
- The integration and automation of security or new tools and practices for the control of cloud-native applications requires more efficient models like DevSecOps and GitOps.
- Business needs regarding sustainability demand new carbon neutrality goals, resulting in additional monitoring activities (like CO2 emissions or power consumption), implementing circularity practices and evolving sourcing processes (e.g., GreenOps).
- The increasing demand to better control cloud spending results in evolving FinOps tools and more advanced cloud financial management processes.

I&O leaders face constant pressure to optimize their IT operating model to satisfy the ever-changing industry requirements and business goals of their organizations. All companies must have an operating model, and it should be maintained and evolved to cover the dynamic gap between the business objectives and how organizations have to operate to achieve them.

This new Hype Cycle for Operating Models provides insight on the level of maturity, relevancy and adoption of some operation patterns, management and governance models that organizations should assess for further developing or adapting to their current IT operating model.

Figure 1: Hype Cycle for Operating Models, 2023



The Priority Matrix

The Priority Matrix maps the time to maturity of a technology/framework on a grid in an easy-to-read format. It answers two high-priority questions:

1. What are the potential benefits and value from an innovation?

2. When will the innovation be mature enough to provide this value?

Transformational innovations are driving operating models and digitalization adoption across IT organizations. These include DevSecOps, NetDevOps, augmented FinOps and platform operating model.

High-priority innovations are helping operating models measure and transition organizations. These include cloud center of excellence, infrastructure orchestration, cloud resilience, FinOps and operational AI systems.

Moderate impact innovations for operating models that are emerging or nascent include CloudOps, multicloud management and GreenOps.

Table 1: Priority Matrix for Operating Models, 2023

(Enlarged table in Appendix)

Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
Transformational	DevSecOps	NetDevOps Platform Engineering	Augmented FinOps Platform Operating Model	
High	Cloud Center of Excellence Product-Centric Delivery Model	Cloud Resilience Cloud Sustainability DataOps FinOps GitOps Infrastructure Automation Infrastructure Orchestration	AIOps Platforms DesignOps Infrastructure Platform Engineering ModelOps Operational AI Systems	YBI YRI
Moderate		CloudOps DevOps Test Data Management Multicloud Management	GreenOps	
Low				

Source: Gartner (July 2023)

On the Rise

GitOps

Analysis By: Paul Delory, Arun Chandrasekaran

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

GitOps is a type of closed-loop control system for cloud-native applications. The term is often used more expansively, usually as a shorthand for automated operations or CI/CD, but this is incorrect. According to the canonical OpenGitOps standard, the state of any system managed by GitOps must be: (1) expressed declaratively, (2) versioned and immutable, (3) pulled automatically, and (4) continuously reconciled. These ideas are not new, but new tools and practices now bring GitOps within reach.

Why This Is Important

GitOps can be transformative. GitOps workflows deploy a verified and traceable configuration (such as a container definition) into a runtime environment, bringing code to production with only a Git pull request. All changes flow through Git, where they are version-controlled, immutable and auditable. Developers interact only with Git, using abstract, declarative logic. GitOps extends a common control plane across Kubernetes (K8s) clusters, which is increasingly important as clusters proliferate.

Business Impact

By operationalizing infrastructure as code, GitOps enhances availability and resilience of services:

- GitOps can be used to improve version control, automation, consistency, collaboration and compliance.
- Artifacts are reusable and can be modularized.
- Configuration of clusters or systems can be updated dynamically. All of this translates to business agility and a faster time to market.

- GitOps artifacts are version-controlled and stored in a central repository, making them easy to verify and audit.

Drivers

- **Kubernetes adoption and maturity:** GitOps must be underpinned by an ecosystem of technologies, including tools for automation, infrastructure as code, continuous integration/continuous deployment (CI/CD), observability and compliance. Kubernetes has emerged as a common substrate for cloud-native applications. This provides a ready-made foundation for GitOps. As Kubernetes adoption grows within the enterprise, so can GitOps, too.
- **Need for increased speed and agility:** Speed and agility of software delivery are critical metrics that CIOs care about. As a result, IT organizations are pursuing better collaboration between infrastructure and operations (I&O) and development teams to drive shorter development cycles, faster delivery and increased deployment frequency. This will enable organizations to respond immediately to market changes, handle workload failures better, and tap into new market opportunities. GitOps is the latest way to drive this type of cross-team collaboration.
- **Need for increased reliability:** Speed without reliability is useless. The key to increased software quality is effective governance, accountability, collaboration and automation. GitOps can enable this through transparent processes and common workflows across development and I&O teams. Automated change management helps to avoid costly human errors that can result in poor software quality and downtime.
- **Talent retention:** Organizations adopting GitOps have an opportunity to upskill existing staff for more automation- and code-oriented I&O roles. This opens up opportunities for staff to learn new skills and technologies, resulting in higher employee satisfaction and retention.
- **Cultural change:** By breaking down organizational silos, development and operations leaders can build cross-functional knowledge and collaboration skills across their teams to enable them to work effectively across boundaries.
- **Cost reduction:** Automation of infrastructure eliminates manual tasks and rework, improving productivity and reducing downtimes, both of which can contribute to cost reduction.

Obstacles

- **Prerequisites:** GitOps is only for cloud-native applications. Many GitOps tools and techniques assume the system is built on Kubernetes (frequently, they also assume that a host of other technologies are built on top of K8s). By definition, GitOps requires software agents to act as listeners for changes and help to implement them. GitOps is possible outside Kubernetes, but in practice K8s will almost certainly be used. Thus, GitOps is necessarily limited in scope.
- **Cultural change:** GitOps requires a cultural change that organizations need to invest in. IT leaders need to embrace process change. This requires discipline and commitment from all participants to doing things in a new way.
- **Skills gaps:** GitOps requires automation and software development skills, which many I&O teams lack.
- **Organizational inertia:** GitOps requires collaboration among different teams. This requires trust among these teams for GitOps to be successful.

User Recommendations

- **Target cloud-native workloads initially:** Your first use case for GitOps should be operating a containerized, cloud-native application that is already using both Kubernetes and a continuous delivery platform such as Flux or ArgoCD.
- **Build an internal operating platform:** This is the foundation of your GitOps efforts. Your platform should manage the underlying infrastructure and deployment pipelines, while enforcing security and policy compliance.
- **Embed security into GitOps workflows:** Security teams need to shift left, so the organization can build holistic CI/CD pipelines that deliver software and configure infrastructure, with security embedded in every layer.
- **Be wary of vendors trying to sell you GitOps:** GitOps isn't a product you can buy, but a workflow and a mindset shift that becomes part of your overall DevOps culture. Tools that expressly enable GitOps can be helpful; but GitOps can be done with nothing more than standard continuous delivery tools that support Git-based automation.

Sample Vendors

GitLab; Harness; Red Hat; Upbound; Weaveworks

Gartner Recommended Reading

Innovation Insight: Top 4 Use Cases for GitOps

Is Using GitOps-Style Automation With Kubernetes Right for Me?

How to Scale DevOps Workflows in Multicluster Kubernetes Environments

Designing and Operating DevOps Workflows to Deploy Containerized Applications With Kubernetes

Automate the Application Delivery Value Stream

Augmented FinOps

Analysis By: Adam Ronthal, Dennis Smith

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

FinOps applies the traditional DevOps concepts of agility, continuous integration and deployment, and end-user feedback to financial governance, budgeting and cost optimization efforts. Augmented FinOps automates this process through the application of artificial intelligence (AI) and machine learning (ML) practices — predominantly in the cloud — to enable environments that automatically optimize cost based on defined business objectives expressed in natural language.

Why This Is Important

In the cloud, it is now possible to assess the cost of a specific workload or collection of workloads assigned to a project. However, price/performance — the primary measure of cloud efficiency — is difficult to assess due to the complexity and diversity of choice in underlying cloud infrastructure and service offerings and a lack of consistency in pricing models. Augmented FinOps can automate this process by applying AI/ML techniques.

Business Impact

The automation of cloud budget planning and financial operations will allow businesses to express their objectives — ideally in natural language — and allow their cloud ecosystems to automatically optimize the underlying cloud resources to meet those objectives. This will result in more efficient use of resources and, therefore, optimal spend by reducing/eliminating misaligned or poor use of cloud infrastructure and service offerings.

Drivers

- Practitioners are increasingly realizing that cloud is fundamentally a complex cost optimization exercise.
- Cloud adopters have a strong desire for transparency into cloud spending.
- Buyer inexperience is leading to either under-provisioning and associated resource contention or overprovisioning and spending more than is needed.
- Vendors are positioning cost-effectiveness as a competitive differentiator in their go-to-market strategies.
- Practitioners need to reduce the unpredictability of cloud spending when using cloud infrastructure and services for analytics, operational database management systems (DBMSs), data lakes and other applications, including custom IT infrastructure.
- Consumption-based usage remains common in earlier stages of cloud adoption, driving the need for augmented FinOps, although commit-based usage mitigates some unpredictability.
- Cost overruns are often obscured, downplayed, or dismissed by line of business implementers, requiring augmentation to achieve holistic and comprehensive cost optimization.
- Automation of financial governance controls in cloud environments provides increased predictability and cost optimization with less operational effort.
- Solid financial governance frameworks are positioning organizations to take advantage of FinOps.
- Emergence of specific roles — like FinOps practitioner or cloud economist — focused on FinOps practices and cost optimization means organizations have the expertise to address augmented FinOps.
- Owing to their complexity, cloud environments are ideally suited for the application of ML and AI methods to automate processes and track price and performance.
- Core FinOps capabilities are being delivered in three ways: Homegrown solutions, cloud service provider (CSP) instrumentation and third-party vendors. Increasingly practitioners are seeking out third-party or CSP tools to address their needs. All of these have a broad objective of adopting augmented capabilities as a means of competitive differentiation.

Obstacles

- Cloud service provider pricing models remain needlessly complex and diverse.
- Cloud ecosystems are (and will remain) open to third-party participants, which implies multiple commercial arrangements with multiple providers.
- Standards for cloud cost, usage and billing data like the FinOps Foundation's FOCUS proposal have yet to be broadly adopted. APIs for communicating performance data within the context of a broader ecosystem have yet to emerge. Both of these are required to assess the primary measure of success: price/performance.

User Recommendations

- Seek out service offerings to automate (via AI/ML) performance, consumption and pricing options. Increasingly, incorporate these capabilities into cloud data ecosystems that will learn from consumption patterns as they seek to optimize the underlying resources, and by extension, cloud spending through orchestration and optimization.
- Apply Gartner's FinOps Maturity Model to assess FinOps offerings in terms of their ability to address the following core capabilities: Observe, report, recommend, predict and optimize. The last three introduce augmented FinOps capabilities.
- Plan to use multiple tools to address the full scope of requirements. Many tools are broad in reach, but do not go deep into prescriptive recommendations. Others are tightly scoped and provide very targeted optimizations. Expect to spend time combining multiple tools to achieve broad and deep capabilities.

Sample Vendors

Acceldata; Anodot; Apptio; Capital One Software; Densify; Enteros; Finout; OtterTune; Sync Computing; Unravel Data

Gartner Recommended Reading

How to Identify Solutions for Managing Costs in Public Cloud IaaS

A Guidance Framework for Selecting Cloud Management Tools

Emerging Tech: Data Management Product Leaders Must Implement Augmented FinOps in Their Cloud Solutions

CDAOs and CFOs Must Drive Business Value in the Cloud Through Collaboration

Financial Governance Is Essential to Successful Cloud Data and Analytics

GreenOps

Analysis By: Miguel Angel Borrega, Autumn Stanish, Philip Dawson

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

GreenOps is an approach that enables IT management and governance under principles and practices for maximizing IT's efficiency, while reducing its environmental footprint. GreenOps leverages metrics like energy consumption, GHG emissions and e-waste generation to place and optimize workloads on IT infrastructure. It also provides the IT strategic planning of development, deployment, resource allocation, and eco-culture required by organizations to achieve their sustainability goals.

Why This Is Important

Organizations have ambitious goals to reduce their environmental footprints. They need a sustainable plan for their future IT and new operations based on "green" metrics and processes, which are rarely present in current IT operations. With the lens of GreenOps, organizations can understand the environmental impacts of their IT strategies, maximize their IT efficiency, and reduce their carbon footprint while simultaneously promoting environmental responsibility at every level of the enterprise.

Business Impact

Sustainability and reduction of operational costs are natural benefits of GreenOps. Being sustainable in IT almost always has a positive impact on company finances. GreenOps helps organizations take more informed sustainable decisions about selecting the right IT providers and partners. GreenOps contributes to reducing investments in carbon offsets, mitigating potential fines from regulators, and increasing the organization's environmental reputation and business profitability.

Drivers

- GreenOps provides the IT strategic planning of development, deployment, resource allocation, and eco-culture required by organizations to reduce the carbon footprint of their IT.
- Eco-conscious designs for new data centers, as well as the energy-efficient technology and operations of public cloud providers, can create up to 90% fewer GHG emissions than traditional and legacy on-premises data centers.
- GreenOps helps analyze IT providers' current environmental sustainability efforts and roadmap to help them avoid getting stuck with the wrong sustainability partner for the long term.
- Public cloud will be central to sustainable IT, as it will help to reduce the organization's carbon footprint by migrating and operating workloads. By adopting GreenOps, organizations follow principles, implement processes and use available tools to determine when cloud services should be used, when they are being used inefficiently, and how to rectify that to cut out waste and achieve the targeted sustainability outcomes.
- GreenOps supports the organization's capability to attract consumers and businesses that are increasingly interested in purchasing from responsible companies with strong ESG principles, by embedding a culture and responsibility for sustainability throughout IT.
- Sustainability is a shared responsibility between external IT providers and organizations. GreenOps supports the commitment to this responsibility within the organization by requiring the company to adopt energy and water efficiency technologies, select clean energy providers and implement circularity processes.
- In the near future, organizations will demand more than just the carbon footprint information of their data centers or IT infrastructure. GreenOps will help get real-time and more granular carbon emissions information at different levels: departments, workloads, applications or even users, by tracking sustainability metrics.

Obstacles

- Environmental sustainability is not yet a priority for many organizations, as their net-zero time commitments are far away.
- The “greenwashing” alternative can be more attractive than implementing sustainable environmental initiatives and operations.
- Few providers understand the relative complexity of IT environmental sustainability. There is a lack of accurate data about how emissions are measured and calculated in IT environments.
- Environmental sustainability tools are still rudimentary. They are mainly based on estimations and not real data.
- Implementing GreenOps requires a comprehensive overview of the environmental impact of every area in IT. IT leaders’ mindsets have to change to become part of the broader conversation on sustainability. Once everyone understands they have a role to play in reducing their carbon footprint, then the organization can start to achieve their combined sustainability and IT goals.

User Recommendations

- Support your organization's environmental sustainability objectives by creating a roadmap that implements IT efficient technologies and processes to reduce your IT carbon footprint.
- Establish your current sustainability performance across all areas of IT to define realistic sustainability goals.
- Commit to sustainability targets and build long-term IT strategies by adopting sustainability metrics and processes designed to make iterative progress toward them.
- Build sustainability skills on your IT operations team by creating common work areas with cloud financial management to make joint decisions.
- Use available tools and resources to manage and optimize your sustainability metrics, eliminate waste and make services more efficient.
- Place workloads in the most efficient platforms by migrating energy-intensive applications.
- Include environmental sustainability as a key decision factor in sourcing by growing through sustainable business models and continuously improving.

Gartner Recommended Reading

Quick Answer: How Green Are Public Cloud Providers?

Build an Environmental Cloud Sustainability Strategy

How to Evaluate Vendor Sustainability

Quick Answer: How Can Sustainability Drive Data Center Infrastructure Cost Optimization?

Unlock the Business Benefits of Sustainable IT Infrastructure

DesignOps

Analysis By: Will Grant, Brent Stewart

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

DesignOps is a set of operational practices that enables design-team management and product-level delivery of design assets. The team management side stresses strategic alignment with business operations for the central design function and career development. The product delivery side combines user experience (UX), product management and technology operations to enable efficient and DevOps-compatible plans, estimates and processes that support quality, collaboration and ongoing innovation.

Why This Is Important

DesignOps introduces formalized approaches to governance, operations and people management. As a set of easy-to-use operational standards, DesignOps continues to gain in popularity. Digital product companies and agencies are discovering the tremendous value of a proven operational approach for UX team management and design delivery on product teams.

Business Impact

DesignOps represents the first widespread implementation of operational methods and techniques created for both designers and developers. DesignOps adds value during the creation and delivery of design assets. DesignOps practices should cover how teams are organized such that they can better support ongoing feature enhancement and idea generation without interrupting the continuous workflow of development teams.

Drivers

- **Innovation:** When coupled with DevOps, DesignOps leads to more innovative solutions. As a practice, DesignOps employs dual-track agile, which sets aside ongoing tracks of work dedicated to new discovery, idea generation and design exploration. This work acts as a constant source of evidence-based, multidisciplinary innovation.
- **Speed:** DesignOps reduces the time to market for major updates and incremental feature enhancements alike. Due to the concepts of continuous discovery and continuous delivery, developers engage in tech design, architectural explorations and proofs of concept (POCs) sooner than before, and with a deeper understanding of the overall vision.
- **Collaboration:** DesignOps increases communication and camaraderie between design and development teams. The design-development gap exists for many reasons, one of them being culture. DesignOps promotes multidisciplinary teams in workshop settings, design sprints or one-on-one "pairing and sharing" that promotes understanding, empathy and relationship building between these two crucially important groups.

Obstacles

- Few UX practitioners are educated in detailed planning and estimation, using a common work breakdown structure (WBS).
- Few product managers are trained in UX planning, estimating and tracking, and many of the design platforms lack robust change control solutions, although this is improving.
- Popular enterprise agile planning (EAP) tools are not designed with UX practitioners, activities and deliverables in mind (although this is changing), leading to resistance from UX teams to adopt tools they perceive as "for developers."

User Recommendations

Software engineering leaders should:

- Encourage design and UX professionals to adopt a DesignOps practice to better manage the complete design life cycle.

- Ensure that the DesignOps practice covers the following three key aspects: how UX teams are organized, the tools and processes for delivering UX artifacts and how success is measured.
- Develop Agile training designed for UX professionals, available as part of the DesignOps practice.
- Determine the value of a DesignOps approach with a pilot program involving an existing high-performing team.

Following a successful pilot, application leaders and the pilot team members should:

- Engage in a productwide rollout that involves training, updated product plans and the allocation of one or more people to the role of design manager.

It should be noted that a successful rollout of DesignOps at the product level requires buy-in from product management, design and development teams, as well as robust logistical and administrative skills.

Gartner Recommended Reading

How Design, Development and Product Management Can Work Together Successfully

The 4 Secrets of Design-Led Companies

2023 Software Engineering Primer: Build and Deliver New Digital Products/Experiences to Drive Business Results

Keys to DevOps Success

NetDevOps

Analysis By: Andrew Lerner

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

NetDevOps entails applying DevOps and/or continuous integration/continuous deployment (CI/CD) practices to networking activities. This requires an automated pipeline that includes staging, pre/postvalidation, and testing of networking activities such as provisioning. Similar terms used to describe this approach include “NetOps 2.0” and “network as code.”

Why This Is Important

NetDevOps can improve agility, reduce toil and increase reliability. It is particularly valuable for organizations implementing infrastructure as code (IaC) for other portions of their infrastructure, because the network is often a bottleneck. We estimate that less than 10% of enterprises actively use NetDevOps practices currently. Thus, there are ample opportunities to further improve agility while reducing human error within network provisioning and ongoing operations.

Business Impact

The use of NetDevOps practices helps to deliver networking functionality to the business faster, and increase overall network uptime, and aid with compliance.

Drivers

- As organizations implement IaC, GitOps and/or DevOps, traditional approaches to network provisioning are not sufficiently agile or reliable. NetDevOps helps to bring the network up to speed with other infrastructure and application processes.
- There is very limited tolerance for network outages/downtime. The practices associated with NetDevOps, such as automated testing, reduce the likelihood of a production impact because of increased testing, peer review, validation and automated rollback.
- NetDevOps practices drive clear workflows and documentation, which helps with auditing and governance, and troubleshooting.
- Network infrastructure and automation vendors are increasingly integrating their workflows with IaC and CI/CD tools, and marketing these concepts.
- For organizations embracing public cloud and cloud-native concepts, networks are typically built and provisioned with the application. Thus, it makes sense to integrate network, infrastructure and app provisioning using the same (or similar) processes.

Obstacles

- Many network teams aren't aware of NetDevOps.
- The skills and expertise required for NetDevOps (i.e., software development practices, Ansible, Terraform, Nornir, Python, APIs) are different from common network engineering skills, and in limited supply.
- NetDevOps requires highly accurate up-to-date network information (inventory, location, etc.), which is uncommon in many enterprises.
- Network teams are risk-averse and lack confidence in automating data center networks, because the business impact of outages are massive.
- There are few commercial network automation offerings that provide multivendor breadth and feature depth across data center, cloud, campus, WAN and security domains.
- Inconsistent or undocumented workflows limit adoption.
- Most enterprises do not have "development" or "test" network environment(s) which prevents or limits the effectiveness of NetDevOps practices.

User Recommendations

- Apply NetDevOps practices opportunistically, including as part of broader IaC practices. NetDevOps is not a fit for all networking activities; don't try to use NetDevOps techniques for all changes.
- Invest in personnel by shifting hiring and training focus toward specific software competencies, including Ansible and Python, community forums and cross-pollinating networking teams with adjacent DevOps personnel.
- Capture and store both device configurations and operational network state (for example, active routing tables) in a version control system.
- Invest in network infrastructure and network automation tools that offer published, open, restful APIs that expose more than 90% of functionality.
- Create standard templates for device types, apply versioning, and track configuration drift.
- Automate pre- and post-change validation, and configuration rollback.
- Automate pre- and post-environmental testing, such as latency/availability checks.

Sample Vendors

Arista; Amazon Web Services; HashiCorp; Itential; Network to Code; Red Hat

Gartner Recommended Reading

Market Guide for Network Automation Tools

The Top 5 Trends in Enterprise Networking and Why They Matter: A Gartner Trend Insight Report

3 Actions to Retain Customers and Grow Revenue in the Enterprise Network Hardware Market

Cloud Sustainability

Analysis By: Ed Anderson

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Cloud sustainability is the use of cloud services to achieve sustainability benefits within economic, environmental and social systems. As such, cloud sustainability refers to both the sustainable operation and delivery of cloud services by a cloud service provider, as well as the consumption and use of cloud services by organizations and individuals to achieve sustainability outcomes.

Why This Is Important

Cloud sustainability is a key digital technology supporting organizations in their use of technology to achieve their sustainability ambitions. Cloud computing models are well-suited to deliver sustainability benefits because of their ability to operate at scale using a shared services model, which results in efficient use of computing resources. Hyperscale cloud data centers can be physically located near renewable energy sources further extending their potential to lessen environmental impact.

Business Impact

Increasing attention and focus on environmental and social issues is motivating organizations to improve their sustainability posture. Pressure from customers, investors, partners, regulators, employees, and the public at large is motivating organizations to establish sustainability goals and to demonstrate sustainability outcomes. Cloud computing has great potential to improve sustainability outcomes through efficient operations and the delivery of cloud-based technology innovations.

Drivers

- Sustainability is a rising imperative for organizations across all industries and in all countries and regions around the world. Although sustainability encompasses environmental, social and economic factors, environmental sustainability receives the most attention.
- Corporate climate and decarbonization commitments are typically cascaded to individual business functions, including IT. Consequently, IT organizations are looking at all possible ways to implement such strategies, including cloud sustainability initiatives.
- Market data shows that customers, investors, regulators, citizens and employees increasingly value organizations with demonstrable commitments to sustainability.
- Sustainability investments correlate with operational efficiency. Most organizations operating in an increasingly sustainable fashion also recognize other benefits such as reduced spending on energy, reductions in waste and improvements in water use.
- Cloud providers, being among the world's largest data center operators, show strong commitments to cloud sustainability and are making demonstrable progress toward delivering sustainable cloud service offerings.
- Regulatory and legislative mandates for sustainability are increasingly common across regions and industries. The use of cloud services and other digital technologies will help organizations comply with future regulatory reporting requirements.

Obstacles

- Sustainability definitions, metrics and reporting standards are inconsistent, varying by region and industry. Defining, tracking and reporting sustainability performance is complex for most organizations.
- Cloud providers claim to have made great strides in offering sustainable cloud solutions, but these claims are often difficult to verify and contribute to potential "greenwashing." The lack of sustainability reporting standards makes it difficult to interpret and validate provider claims.
- Achieving cloud sustainability outcomes is a shared responsibility between the cloud provider and the customer. Cloud providers must demonstrate sustainable cloud operations, and cloud consumers must employ sustainability practices in their use of cloud services.
- Renewable energy is a key enabler of cloud sustainability and yet there is insufficient capacity to generate and store the energy required to meet the needs of the world's cloud service offerings.

User Recommendations

- Establish internal sustainability goals including specific metrics and sustainability outcomes by doing a materiality assessment to determine which sustainability outcomes are most important to your organization.
- Determine the role cloud sustainability will play in the achievement of sustainability outcomes. Build internal credibility for cloud sustainability by ensuring that the sustainability benefits of specific cloud service offerings are independently validated.
- Engage relevant executives and other internal stakeholders proactively that are tasked with creating and achieving sustainability goals. Establish credible metrics for measuring and reporting cloud sustainability outcomes.
- Look to cloud providers and other experts, including IT service providers, for best practices in operating and consulting cloud services in a sustainable manner.

Sample Vendors

Alibaba Cloud; Amazon Web Services; Google; IBM; Microsoft; Oracle; Salesforce; SAP; Scaleway; VMware

Gartner Recommended Reading

Executive Leadership: Sustainability Primer for 2023

Quick Answer: How Green Are Public Cloud Providers?

Build an Environmental Cloud Sustainability Strategy

Make Sure Technology Helps More Than Hurts Sustainability

Sustainability: A Customer Priority and Provider Imperative

FinOps

Analysis By: Lydia Leong

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

FinOps is the model proposed by the FinOps Foundation to implement cloud financial management (CFM). FinOps applies DevOps principles and practices to cloud financial operations. The FinOps Foundation defines FinOps (which it has trademarked) as "an evolving cloud financial management discipline and cultural practice that enables organizations to get maximum business value by helping engineering, finance, technology and business teams to collaborate on data-driven spending decisions."

Why This Is Important

All organizations with meaningful spend on cloud IaaS or PaaS need to engage in cloud financial management (CFM) so that they are aware of what they are spending and why. Organizations must undertake greater cost governance efforts if they have substantial spending, significant self-service, cost complexity or variability. Further, CFM helps organizations optimize their costs and extract greater value from their spending. FinOps is one possible implementation model for CFM.

Business Impact

FinOps is a partial solution to CFM needs. Cloud economics spans the continuous process of CFM as well as one-off activities, and is focused on maximizing the value of cloud computing to the business, rather than minimizing cloud expenses. For example, business leaders may reasonably make the decision to spend more to deliver a better user experience, or to ignore cost-related technical debt so application teams can focus on delivering more features.

Drivers

- Public cloud costs are of concern to many customers. Many customers experience unexpectedly high cloud costs because they have fulfilled far greater business demand for cloud services than the IT organization had forecast.
- Ungoverned cloud adoption can lead to uncontrolled and careless spending. Organizations without an effective CFM practice cannot properly plan, track or optimize their cloud costs.
- Organizations that do not effectively manage cloud economics cannot assist the business in making thoughtful decisions about the top line versus the bottom line in cloud-enabled digital products and services.
- The FinOps Foundation (FOF), founded in 2019 by several cloud cost management tool vendors, created and popularized the use of the FinOps term. At that time, it defined FinOps as “the practice of bringing financial accountability to the variable spend model of cloud, enabling distributed teams to make business trade-offs between speed, cost and quality.”
- FOF changed the definition of FinOps in November 2021. The new definition is more closely aligned to Gartner’s recommended practices for the management of cloud economics. However, not all entities use the FinOps term in a consistent way.
- In mid-2020, FOF became a project of the Linux Foundation. Its membership has grown over time, and now includes many vendors that sell FinOps tools and services (which FOF will badge as FinOps Certified Platforms), numerous cloud providers, several global systems integrators and some enterprises (mostly financial services institutions). These members promote FinOps concepts to their users, increasing hype.
- FOF has consistently promoted the adoption of a centralized FinOps team, which in turn purchases and uses FinOps tools, leading customers to believe they should adopt this approach.
- FOF launched the FinOps Open Cost Usage Specification (FOCUS) in 2023. It is intended to be an open standard for cloud billing data, and will be broadly useful if widely adopted by cloud providers.

Obstacles

- Not all organizations have a business case for CFM, although almost all organizations that have meaningful cloud adoption need to perform cost management.
- CFM needs to be a cross-functional and cultural practice, not solely the responsibility of a dedicated FinOps team. In addition, many organizations cannot cost-justify having such a team.
- Application teams and the business owners of applications need motivation to optimize their cloud spend. This usually requires coupling showback to incentives (or penalties) or performing chargeback, forcing these entities to be accountable for what they spend.
- Although FinOps tools can often recommend optimizations for cloud infrastructure, they have limited capabilities for PaaS.
- Many organizations do not undertake activities that reduce their cloud spending because these activities do not have an adequate ROI. That is, the spend reduction is insufficient to justify the time and labor necessary to technically implement the optimizations.

User Recommendations

- Establish a cross-functional CFM practice — not just a FinOps team — once you have public cloud IaaS and PaaS adoption that has proceeded beyond the pilot stage.
- Your cloud center of excellence (CCOE) or other cloud governance function should own the CFM practice. The CCOE should set the policies and guidance, but cloud operations teams are typically responsible for implementing CFM tools and assisting application teams with optimizations.
- When custom-developing cloud solutions, design cost-aware architecture. Application design and implementation will be the primary influence on cloud costs.
- When migrating existing applications to the cloud through a lift-and-shift (that is, a rehost) approach, use performance-based rightsizing and accept the smallest recommended size by default. Most organizations tend to oversize virtual machines when they migrate, due to unwarranted concerns about performance and “headroom.”

Sample Vendors

Apptio; Flexera; VMware

Gartner Recommended Reading

Is FinOps the Answer to Cloud Cost Governance?

Managing Cloud Economics: A Cloud Architect's Guide to Productive Relationships With Sourcing Leaders

Effective Cloud Sourcing Strategies Focus on FinOps, Not Cost Reductions

Beyond FinOps: The Gartner Framework for Public Cloud Financial Management

Infrastructure Orchestration

Analysis By: Chris Saunderson

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Infrastructure orchestration (IO) enables platform and I&O teams to design, deliver, operate and ensure orchestrated services across on-premises, cloud and edge deployments. IO enables templated service creation and management, spanning provisioning, Day-2 operations and integration with CI/CD, self-service portals, and API access to orchestrated services.

Why This Is Important

Infrastructure orchestration provides strategic workflow capabilities to drive life cycle delivery and ongoing maintenance of complex deployed infrastructure. These practices and tools enable agile, iterative automation delivery and execution of the processes required via self-service and API access. This investment improves the velocity and quality of infrastructure services, improves traceability and visibility of service delivery and reduces inconsistencies from manual activities.

Business Impact

Infrastructure orchestration drives consumer experience improvements of deploying and managing standardized infrastructure. I&O teams realize operational efficiencies through reduced manual efforts to deliver infrastructure, embedding security and compliance requirements into the delivered services, and offering cost optimization opportunities. I&O staff can transform their role into an automation-first focus and scale to meet increased business demands.

Drivers

- **Business agility:** Organizations must increase responsiveness to meet customer needs and adapt to market and technology changes. They must be able to deliver products that meet these changing demands and requirements quickly.
- **Cost optimization:** Infrastructure teams leverage orchestration to deliver scalable, reliable and secure platforms. This helps to improve delivery efficiency, reduce human work, and reduce downtime due to change failures.
- **Value extraction:** adoption of orchestration capabilities unlocks additional value from the automation tools already implemented, enabling incident response, request servicing and other tasks to be more richly automated and consumed.
- **DevOps:** Infrastructure orchestration is a key enabler of continuous software delivery, allowing the DevOps team to automate the provisioning and management of environments.
- **Infrastructure complexity:** Increasingly complex deployment topologies require greater automation to improve the consumability of infrastructure and the ongoing maintenance of deployments,
- **Security and compliance:** Increased automation enables the implementation of security and compliance controls through orchestration and avoids any audit failures. The end-to-end visibility and traceability of the provisioning and configuration can enable continuous compliance automation of the infrastructure.

Obstacles

- **Skill development:** Infrastructure orchestration practices and tools can be complex to implement and sustain, as they require skills beyond scripting to get maximum value. These tools leverage software engineering skills that can be challenging to find in I&O teams.
- **I&O operating models:** The organizational structure of many I&O teams is set up by domain specializations, making it hard to develop and deliver end-to-end services through orchestration. Perceptions of stability and reliability risks slow adoption.
- **Automation constraints:** To automate maintenance activities, a certain level of maturity needs to be reached within the organization. Orchestration requires that automated tasks be available to be able to realize maximum return on investment.

User Recommendations

- Identify and catalog use cases and constraints in your delivery workflows that are injecting delay into service delivery, especially for tasks that are executed manually.
- Benchmark existing service delivery execution time and quality problems to measure against to demonstrate improvement.
- Catalog operational tasks that are being executed manually today and are candidates to develop workflows to implement.
- Identify candidate orchestration platforms to execute proof of value testing with, ensuring that the candidates can be integrated into your existing operational environment.
- Monitor implementation to identify successes and opportunities for improvement and build a success story demonstrating velocity, quality, throughput and operational improvements.

Sample Vendors

Cloudsoft; Crossplane; Dell Technologies; env0; Itential; Morpheus Data; PagerDuty; Pliant; RackN; SpaceLift

Gartner Recommended Reading

Innovation Insight for Continuous Infrastructure Automation

To Automate Your Automation, Apply Agile and DevOps Practices to Infrastructure and Operations

Market Guide for Infrastructure Automation Tools

Market Guide for Continuous Compliance Automation Tools in DevOps

Operational AI Systems

Analysis By: Chirag Dekate, Soyeb Barot, Sumit Agarwal

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Operational AI systems (OAISys) enable orchestration, automation and scaling of production-ready and enterprise-grade AI, comprising ML, DNNs and Generative AI. OAISys integrates DataOps, ModelOps, MLOps and deployment services to deliver enterprise-grade governance, including reusability, reproducibility, release management, lineage, risk and compliance management, and security. It also unifies development, delivery (hybrid, multicloud, IoT) and operational (streaming, batch) contexts.

Why This Is Important

OAISys can help enterprises:

- Standardize, govern and automate AI engineering and deployment technologies, and accelerate productization of AI.
- Eliminate system integration friction and impedance mismatch across DataOps, ModelOps, MLOps, deployment and governance platforms.
- Scale AI initiatives by enabling orchestration across hybrid, multicloud, edge AI or IoT.
- Enable discoverable, composable and reusable AI artifacts (data catalogs, feature stores, model stores) across the enterprise context.

Business Impact

OAISys deliver production AI systems that:

- Systemize analytics and AI engineering technologies, including ModelOps and MLOps platforms.
- Integrate existing data, analytics and DSML platforms.
- Utilize reusability components including feature and model stores, monitoring, experiment management, model performance and lineage tracking.
- Homogenize governance including compliance, risk, security, and cost across deployment (hybrid, multicloud, IoT) and operational (streaming, batch) contexts.

Drivers

- Enable business stakeholders to leverage AI as a service that is customized to their enterprise context.
- IT leaders need to deliver, manage and govern AI models within enterprise applications deployed across multiple contexts and jurisdictions (hybrid, multicloud, edge AI and IoT).
- Traditional siloed approaches of data management and AI engineering create integration challenges across the data ingest, processing, model engineering and deployment.
- OAISys enables enterprises to standardize and automate development, management, deployment, maintenance and governance technologies to deliver comprehensive, flexible and composed end-to-end AI systems.
- It helps align and automate the data, AI model deployment and governance pipelines.
- Operationalization and automation platforms are a core part of how early enterprise AI pioneers scale productization of AI by leveraging existing data, analytics and governance frameworks.
- Standardizing data pipelines, including DataOps toolchains, creating reusability components such as data catalogs and ETL registries, monitoring, security, access control and lineage tracking.
- The enterprise OAISys enables unification of two core contexts: deployment context across hybrid, multicloud, edge AI and IoT, and operational context across batch and streaming processing modes that commonly occur as enterprises train and deploy production models.

Obstacles

- Enterprises with low data and AI maturity levels will find OAISys intimidating to build, deliver and support.
- OAISys requires integration of full-featured solutions with select tools that address portfolio gaps with minimal overlap. These include capability gaps around feature stores, model stores, governance capabilities and more.
- OAISys requires a high degree of cloud maturity, or the ability to integrate data and model pipelines across deployment contexts. The potential complexity and costs may be a deterrent for organizations just starting their AI initiatives.
- Enterprises seeking to deliver OAISys often seek “unicorn” experts and service providers to productize AI. Fully featured vendor solutions that enable OAISys are hard to come by, and enterprises often have to build and support these environments on their own.

User Recommendations

- Focus AI engineering activities to deliver business context customized operational AI systems.
- Rationalize data and analytic environment and leverage current (simplified subset of) investments in data management, DSML, ModelOps and MLOps tools to build OAISys.
- Leverage cloud service provider environments as foundational environments to build OAISys along with rationalizing your data, analytics and AI portfolios as you migrate to the cloud.
- Avoid building patchwork OAISys that integrate piecemeal functionality from scratch (and add another layer of tool sprawl). Utilize point solutions sparingly and surgically to plug feature/capability gaps in fully featured DataOps, MLOps and ModelOps tools.
- Actively leverage your existing data management, DSML, MLOps and ModelOps platforms as building blocks, rather than starting from scratch.

Sample Vendors

Amazon Web Services; Dataiku; DataRobot; Domino Data Lab; Google; HPE Ezmeral Software; IBM; Iguazio; Microsoft; ModelOp

Gartner Recommended Reading

2023 Planning Guide for Analytics and Artificial Intelligence

Emerging Tech Impact Radar: Data and Analytics

Quick Answer: How Should CXOs Structure AI Operating Models?

At the Peak

Cloud Resilience

Analysis By: Lydia Leong

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Cloud resilience is the application of resilience principles and practices to the delivery and consumption of cloud services. Resilient systems limit the impact of, and recover quickly from, failure. The shared responsibility model of cloud computing applies to cloud resilience responsibilities.

Why This Is Important

Organizations increasingly wonder if their cloud providers are adequately resilient and what customers should do to mitigate associated risks. However, many cloud customers do not choose more resilient, but higher-cost options when purchasing SaaS. They also do not pay adequate attention to the resilient design, implementation or operations of their applications deployed in infrastructure as a service (IaaS) and platform as a service (PaaS).

Business Impact

Cloud outages may create application downtime, which may have a negative impact on application users, business processes or an organization's customers. Lengthy cloud failures may pose a business continuity risk for inadequately prepared cloud customers. Furthermore, many organizations may be impacted by a cloud outage without being a direct customer of that provider, since cloud services are now often used in many solutions delivered to businesses and individuals.

Drivers

- As public cloud providers grow ever larger and more strategic, they become a systemic risk. Thus, governments and industry regulators are growing more concerned about cloud resilience, and may take actions to address perceived risks.

- Cloud providers have become an integral part of driving the global economy, as well as a critical dependency for ordinary people living their daily lives. Cloud-based identity — including social identity from companies such as Apple, Meta and Google — is used for authentication into many consumer and business applications, websites, and other digital products and services.
- As organizations increase their dependence on cloud services for mission-critical business solutions, they become more concerned about the potential impact of major cloud outages.
- Most organizations are adopting a strategic cloud provider that is the focus of their cloud adoption efforts, thus concentrating more of their application portfolios in a single provider. This increases concerns about availability and business continuity risks, and thus cloud resilience.
- Digital products and services often need continuous availability. Therefore, traditional notions of acceptable maintenance downtime, occasional outages and lengthy manually performed disaster recovery efforts are unacceptable for these solutions.
- Cloud providers deliver public assurances of their resilience, but most offer little transparency into how they accomplish that resiliency. Therefore, organizations may place unwarranted trust in marketing promises or service-level agreements.
- It is easier to blame cloud providers for failures than to look inward. Many organizations that purchase cloud IaaS and PaaS do not understand how cloud failures differ from on-premises data center downtime, and hence do not understand how to properly implement cloud resilience.

Obstacles

- Many organizations question whether it is necessary to spend more money on cloud resilience, given that most cloud providers are quite reliable. Customers often do not understand the resilience-related differences between providers.
- Cloud resilience depends on the appropriate physical and logical design of solutions, implementation quality, the quality of change management, and the quality of the design and execution of both proactive and reactive operations processes.
- A smaller cloud provider may be less able to invest in efforts to become more resilient, and is therefore riskier. However, it may be the sole source of a niche solution, forcing customers to consider their risk appetites.

- Cloud services make it easier to rapidly deliver and update applications. However, application release velocity and operational safety are often in conflict, and cloud self-service capabilities can make it harder to govern application resilience.

User Recommendations

- Adopt a holistic view of potential avenues of system failure, addressed both systemically and for individual applications. Many organizations mistakenly focus only on potential infrastructure problems.
- Create tiered architectural standards based on cloud provider resilience capabilities and limitations. Map application criticality classifications to these tiers. Enforce those standards when sourcing or building cloud solutions.
- Apply site reliability engineering (SRE) principles to improve the resilience of fast-changing applications. You do not need to implement an SRE team to usefully adopt SRE principles.
- Use chaos engineering to test complex cloud solutions. The market-leading cloud IaaS and PaaS offer chaos engineering services that simulate a variety of cloud service failures.
- Optimize your risk assessment and triage efforts when evaluating SaaS providers. Ensure SaaS application owners explicitly acknowledge and accept the risks of such providers.

Gartner Recommended Reading

Designing Availability and Resilience for Applications in Public Cloud IaaS and PaaS

9 Principles for Improving Cloud Resilience

Quick Answer: How Should Executive Leaders Plan for Cloud Outages?

How to Establish Effective SaaS Governance

How to Manage Concentration Risk in Public Cloud Services

YBI YRI

Analysis By: Lydia Leong

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

"You Build It, You Run It" (YBI YRI) is a delivery model that makes application teams (application developers and maintainers) accept principal responsibility for the production operations of their applications, rather than relying primarily on the infrastructure and operations (I&O) team. In this DevOps approach intended to maximize release velocity and application team autonomy, application teams are held accountable for the quality and stability of their applications.

Why This Is Important

The YBI YRI model ensures that developers stay in contact with the day-to-day operations of the software that they build and maintain. It directly exposes them to the customer impact of system failures and performance problems. This motivates them to deliver higher-quality and more resilient software. However, to prevent excessive cognitive load on developers, I&O must be able to support application teams with robust and reliable platforms that reduce the operational burden of this model.

Business Impact

YBI YRI is a delivery model that allows application teams (defined broadly, including business fusion teams, agile product teams and other value-stream-aligned teams) to maximize their release velocity — and thus deliver capabilities more quickly to customers and accelerate the achievement of desired business outcomes. It also drives greater intimacy between developers and customers by making developers more aware of the operational consequences of their decisions.

Drivers

- The phrase “You Build It, You Run It” dates back to a 2006 ACM Queue interview with Amazon’s CTO, Werner Vogels, in which he explained the benefits that had resulted from Amazon’s adoption of a strict service-oriented architecture. In Amazon’s model, each service has an associated team that is completely responsible for that service end to end, including both building and operating the service. This model is sometimes alternatively called “You Build It, You Own It.”
- In the past 15 years, the YBI YRI model has been predominantly an approach taken by digital-native organizations. This has often been driven by necessity, as early-stage startups may not be able to afford to hire a dedicated I&O team, requiring the developers to take on these responsibilities.
- More recently, the growing hype around this approach has influenced ambitious enterprises that are pursuing digital transformation. Such enterprises often want to model themselves after digital-native companies.
- An increasing number of organizations are using the Team Topologies approach to model team structures and interactions. In this approach, stream-aligned teams own a piece of a business domain (or other flow) from end to end, and are therefore YBI YRI teams.
- Although few enterprise applications require the exceptionally high release velocities facilitated by YBI YRI, a growing number of enterprises have at least one application that could potentially benefit from this approach. That application is typically aligned to a digital product or service.
- More organizations that are migrating to the public cloud want to emphasize a self-service approach for application teams using the cloud. Such organizations sometimes wrongly assume that the self-service capabilities available in cloud IaaS and PaaS mean that there is little to no need for the organization to continue to have an I&O team (other than for on-premises infrastructure).

Obstacles

- Most organizations do not have the robust DevOps practices required to successfully adopt YBI YRI, which is a model that distributes responsibility between application teams and I&O teams. Application teams assume responsibility for most of the elements of the application life cycle, with minimal (but still vital) support from central I&O.
- Most organizations do not have secure, stable self-service platform services that enable application teams to operate independently with minimal support or assistance from a central operations function. Even if those platform services are delivered via the public cloud, they still require an appropriate overlay of governance, management, and security.
- Most application teams do not have the staffing scale and skills necessary to competently and safely perform operational responsibilities. Most organizations are reluctant to invest to enable the YBI YRI model.

User Recommendations

- Structure the division of responsibilities carefully when adopting YBI YRI. Do not simply abandon application teams to operational responsibilities and hope for the best. Adopting YBI YRI in the enterprise requires significant preparation work and transition time. Do not assume that the execution of a cloud migration will automatically prepare application teams for YBI YRI.
- Adopt a YBI YRI model only for applications that belong to teams that want to embrace the model, need to frequently deliver working software (solutions) and are willing to accept greater operational responsibilities to accelerate their release velocity.
- Document and manage the risks of adopting a YBI YRI model carefully when the organization does not have mature DevOps adoption, operations and security skills embedded in application teams, or robust platform engineering capabilities. This includes circumstances under which an application team has adopted this model as a result of a public cloud pilot project.

Gartner Recommended Reading

Introducing the “You Build It, You Run It” Modern Operations Pattern

Why DevOps Success Requires Platform Teams

Use Platform Engineering to Scale and Accelerate DevOps Adoption

Comparing Cloud Operations Approaches

Organize for Agility With Team Topologies

Infrastructure Platform Engineering

Analysis By: Hassan Ennaciri, Paul Delory

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Infrastructure platform engineering is the discipline of building internal software products that present IT infrastructure to users or other platforms in an easily consumable way. Infrastructure platforms are self-service tools that allow nonexpert users to deploy and manage infrastructure themselves while I&O retains governance, security and compliance. Infrastructure platforms are often used as the foundation of higher-order, self-service layers such as internal developer platforms.

Why This Is Important

Digital enterprises are pressured to innovate and deliver products faster to meet customer needs. This requires adopting new operating models and modern practices to deliver scalable, reliable platforms that enable faster product delivery. Infrastructure platform engineering provides automated delivery of curated secure, reliable and scalable infrastructure services that can be available via self services or APIs and reduce the effort and cycle time for users to request and access the products.

Business Impact

Infrastructure platform engineering abstracts the complexity of the digital infrastructure to deliver platforms that continuously evolve to meet customer needs. It is an agile approach necessary to enable software products' value streams to meet customer needs and expectations. It also provides on-demand, fast access to environments, services and tools that improve customer experience and productivity.

Drivers

- **Business agility and innovation:** Digital businesses are required to be responsive to customers' needs and changing market conditions. They must have the ability to quickly deliver products that meet these changing demands and requirements.
- **Cost optimization:** Infrastructure platform engineering teams leverage automation to deliver scalable, reliable and secure platforms. This helps to improve efficiency, reduce resource cost due to manual work and reduce downtime due to change failures. Standardizing tools and platforms also optimizes resource utilizations and reduces cost incurred in tool proliferation.
- **Digital infrastructure and platform complexity:** Public cloud IaaS and PaaS deliver extensive capabilities and are designed to be consumable by developers, but most enterprises need additional governance and management that is best delivered by a platform engineering team.
- **Improve developer experience and productivity:** Infrastructure platform engineering abstracts complexity from developers and provides them with quick access or self-service in the environments they need to develop and test their software. Services can be made via an internal developer portal (IDP) such as Backstage, Calibo or Humanitec.
- **Compliance and security:** Infrastructure platform engineering automates and integrates compliance and security controls into software delivery pipelines, improving the organization's security posture and reducing the burden from developers.

Obstacles

- **Confusion:** There is a lot of hype and confusion about platform engineering and what it means. Many vendors are defining it to help sell their products, causing uncertainty with teams trying to adopt it.
- **Cultural:** This operating model is a new, modern approach that requires a shift in how teams work and collaborate, which is the hardest obstacle to overcome for many organizations.
- **Lack of skills:** Infrastructure platform engineering requires software engineering and specialized skills that may not exist in the organization.
- **Structure of traditional I&O operating models:** The organizational structure of many I&O teams is set up by domain specializations, making it hard to develop and deliver end-to-end services.
- **IT service management approaches:** The current approaches are process-heavy and rely on tickets and handoffs.
- **Complexity:** Successful implementation of infrastructure platform engineering is challenging because it requires new roles and involvement from many stakeholders.

User Recommendations

- **Start small and evolve:** Define initial goals and objectives of the platform by understanding common user needs and delivering viable products that continuously evolve to meet those needs.
- **Build a dedicated team with the right skills:** Successful infrastructure engineering practice requires dedicated teams with diverse skills in infrastructure platforms and software engineering.
- **Identify and fill critical roles such as platform owner and platform architect.** Acquire new talent with the required technical skills, the right mindset and strong interpersonal skills. Develop existing resources by provisioning continuous learning opportunities.
- **Adopt a product mindset:** Thread platform users as customers and ensure that you talk to them and continuously get their feedback to meet their existing needs as well as anticipate their future needs. Enable users and reduce the level of effort required to use the platform products.

Gartner Recommended Reading

Adopt Platform Engineering to Improve the Developer Experience

Top Strategic Technology Trends for 2023: Platform Engineering

Innovation Insight for Internal Developer Portals

Quick Answer: How Can I Optimize the Use of Programmable Platforms for Effective Software Delivery?

Guidance Framework for Implementing Cloud Platform Operations

Platform Engineering

Analysis By: Bill Blosen, Paul Delory

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Platform engineering is the discipline of building and operating self-service developer platforms for software development and delivery. A platform is a layer of tools, automations and information maintained as products by a dedicated platform team, designed to support software developers or other engineers by abstracting underlying complexity. The goal of platform engineering is to optimize the developer experience and accelerate delivery of customer value.

Why This Is Important

Digital enterprises need to respond quickly to customer and internal demands; therefore, flexible, complex distributed software architectures have become popular. Software product teams struggle to focus on features due to this complexity, which results in poor developer experience. Platform engineering provides a self-service, curated set of tools, automations and information driven by developer priorities to accelerate value delivery in line with internal stakeholders, such as security and architecture.

Business Impact

Platform engineering empowers application teams to deliver software value faster. It removes the burden of underlying infrastructure construction and maintenance and increases teams' capacity to dedicate time to customer value and learning. It makes compliance and controls more consistent and simplifies the chaotic explosion of tools used to deliver software. Platform engineering also improves the developer experience, thus reducing employee frustration and attrition.

Drivers

- Scale: As more teams embrace modern software development practices and patterns, economies of scale are created, whereby there is enough value to justify creating a platform capability shared by multiple teams.
- Cognitive load: Adoption of modern, distributed architectural patterns and software delivery practices means that the process of getting software into production involves more tools, subsystems and moving parts than ever before. This places a burden on product teams to build a delivery system in addition to the actual software they are trying to produce.
- Need for increased speed and agility: The speed and agility of software delivery is critical to CIOs. As a result, software organizations are pursuing DevOps which is a tighter collaboration of infrastructure and operations (I&O) and development teams to drive shorter development cycles, faster delivery and increased deployment frequency. This will enable organizations to respond immediately to market changes, handle workload failures better and tap into new market opportunities. Platform engineering can drive this type of cross-team collaboration.
- Emerging platform construction tools: Many organizations have built their own platforms, but to date, these platforms have been homegrown, individual efforts tailored to the unique circumstances of the organizations that build them. Platforms generally have not been transferable to other companies or sometimes even to other teams within the same company. However, a new generation of platform-building tools is emerging to change that.
- Infrastructure modernization: During digital modernization, some forward-looking I&O teams embrace a new platform engineering role as a way to deliver more value, increasing their relevance to the business.

Obstacles

- Lack of skills: Platform engineering requires solid skills in software engineering, product management and modern infrastructure, all of which are in short supply.
- Platform engineering is easily misunderstood: Traditional models of mandated platforms with limited regard for developer experience can easily be relabeled and thus not achieve the true benefits of platform engineering.
- Outdated management/governance models: Many organizations still use request-based provisioning models. Those need to give way to a self-service, declarative model, with the primary focus being the effectiveness of the end users developing and operating solutions using the platform.
- Internal politics: There are many intraorganizational fights that could derail platform engineering. Product teams may resist giving up control of their customized toolchains. There might also be no appetite to improve the developer experience. Enterprises may also refuse to fund platform engineering without a clear ROI.

User Recommendations

- Start small with cloud-native workloads: Begin platform-building efforts with thinnest viable platforms for the infrastructure underneath cloud-native applications such as containers and Kubernetes.
- Embed security into platforms: Enable shift-left security within DevOps pipeline platforms, which will provide a compelling paved road to engineers.
- Don’t expect to buy a complete platform: Any commercially available tool is unlikely to provide the entirety of the platform you need. Thus, the job of the platform team is to integrate the components necessary for the platform to meet your needs.
- Implement a developer portal as part of your platform: An internal developer portal (IDP) serves as the user interface that enables self-service discovery and access to internal developer platform capabilities. Consider Backstage open-source or other commercial tools. Note: “IDP” has multiple meanings in this context, as well as in the industry.

Gartner Recommended Reading

How to Start and Scale Your Platform Engineering Team

Guidance Framework for Implementing Cloud Platform Operations

Adopt Platform Engineering to Improve the Developer Experience

Innovation Insight for Internal Developer Portals

Platform Operating Model

Analysis By: Amresh Nandan, Susan Welsh de Grimaldo

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

A platform business is when organizations enable value creation through interactions between people, businesses and things. A platform operating model is a way for communications service providers (CSPs) to deliver value derived, in part, from the ecosystem. It is a practice that delivers value by enabling ecosystem participants, as providers and customers, to enable the creation, exchange and consumption of services.

Why This Is Important

CSPs face intense pressure to create and deliver new and differentiating value. With traditional operating models, the organization delivers most value through its products and services. Platform operating models push CSPs to implement composable infrastructure, leading to agility and flexibility and enabling ecosystem collaboration. As such, CSPs can derive value from the broader ecosystem, and can extend value creation with networking, connectivity, content, collaboration and commerce opportunities.

Business Impact

Platform operating models provide CSPs with major benefits:

- Ability to participate in digital ecosystems as leaders, partners, founders, providers and consumers.
- Prevent networks from becoming a pure connectivity utility.
- Enable CSPs to diversify and create new and distinct value in adjacent markets.
- Accelerate digital business by transforming the information and technology (I&T) operating model.

- Rapidly scale growth utilizing networking effects, agile experimentation with new technologies, and validation of applications, market and industry fit.

Drivers

- The commoditization of CSPs' traditional value streams, such as connectivity, voice and networking, is driving CSPs to consider value creation with content, collaboration and commerce. To do so, they are considering various platform operating models to expand into adjacent markets.
- Digitally enabled powerhouses — such as the digital dragons, Amazon, Apple, Microsoft, Alibaba Group and Google — are already challenging and eroding CSPs' traditional value enablement in infrastructure and connectivity. In response, CSPs are adopting digital platform models and collaborating with digital dragons to find new revenue opportunities for their traditional services, as well as create net new differentiating value.
- CSPs are subject to disintermediation and disaggregation by nontraditional market entrants, including some from adjacent industries. This has resulted in intensified competition, collaboration and "co-opetition," creating the urgent need for a new view of value creation and delivery of new communications services that require ecosystem participation and scale. The ability to create new value beyond convenience and price, by adopting the four types of platform business models (matching, creation, orchestration and collaboration) through B2B2X, requires the implementation of platform operating models.
- If tech leaders do not adopt a platform operating model in the next two to five years, they will be at the risk of being substantially sidelined, and miss out on new and emerging opportunities. Those that do not build such a model will eventually be forced to compete on price and scale, ultimately becoming irrelevant to customers beyond connectivity.
- Adoption of the platform approach to service design and orchestration improves operational efficiencies and moves toward a factory approach (industrialization and repeatability of business solutions and offerings).

Obstacles

- Lack of proactive collaboration between network, IT, business leaders and partners.
- Rigid business and technology operating models.
- Rigid governance — command-and-control process priorities over autonomy and embedded, data-driven decision making.
- Traditional mindset that emphasizes rules and protective governance (99.999% reliability at all costs) over adaptability and learning.
- Siloed approach to value creation and technology platform development.
- Point-to-point integrations.
- Complexities of legacy systems and technologies.
- Lack of a coherent approach to the technology strategy between network and IT.
- Focus on monetizing CSP customers instead of monetizing network assets.

User Recommendations

- Proactively explore value exchange enabled in digital ecosystems by collaborating with business leaders to develop platform business models utilizing all the possibilities that digital ecosystems offer. Explore participation as founders, leaders, providers or consumers.
- Identify potential business opportunities that platform business offers by uncovering relationships, roles and potential for shared capabilities.
- Develop and implement your infrastructure capabilities that enable the utmost open collaboration with various ecosystem players (such as developers, hyperscale digital players and digital natives) by adopting DevOps and agile principles, as well as open APIs and composability principles.
- Accelerate innovation and new value creation and digital transformation by aligning your I&T operating model elements and capabilities to enable business outcomes.
- Start implementing the key elements of an I&T operating model for a flexible and composable future with other technology leaders.

Gartner Recommended Reading

A Visual Guide to Digital Ecosystems

Top Technology Trends for CSPs in 2022: Intelligent Digital Ecosystems

Top Technology Trends for CSPs in 2022: Composable Networks Drive Business Agility

Routes to the Future for CSP CIOs: Invest in Platform Capabilities to Shape Business

Analytics Governance

Analysis By: Andrew White, Kurt Schlegel

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Analytics governance is the setting and enforcement of D&A governance policy along the analytics pipeline, from data discovery through analytics deployment, and access to the analysis and insight. Though the markets use the term “governance” here, what is being delivered by technology vendors is not related to policy setting or enforcement, but execution of policy along the analytics pipeline. A more appropriate name would be analytics stewardship.

Why This Is Important

With increasing interest in analytics and AI, the shift to cloud, and the increased risk from failure and exposure to regulatory controls, the interest in governance along the entire analytics pipelines has ballooned. Unfortunately, there is a huge misunderstanding in the market. What needs to take place in the analytics pipeline is the same as what takes place upstream in operational systems. As few people understand this, hype and confusion reign, and redundant investments exist.

Business Impact

Organizations that balance investments between the latest analytics, BI and data science technology and the needed support for governance will get a greater return on both investments. With the right business outcome and adaptive governance focus, the least amount of mission-critical data and analytics will be governed. This would assist with trusted and reliable analysis and insight leverage.

Drivers

- 2023 is marked with wide data, “lakehouses,” data and analytics producers, data fabrics, and data mesh. At the same time, the analytics pipeline is stretched across organizations and clouds. Complexity and confusion is a big driver of analytics governance.
- A shift in focus from truth to trust in governing data and analytics assets, as the vastness of data can no longer be managed with current truth-based (i.e., yes/no) approaches.
- Increase in demand and deployment of self-service analytics and BI, and more rapid prototyping of analytics outputs by users closer to the point of decision.
- The interest and need to govern data inbound to a data warehouse or lake, to have access to that data in the analytics development, and to model, share and create new analytics.
- More complex organizational structures lead to increased demand, whereby various works of data, analytics or governance are widely distributed across business units, business functions, fusion teams, and IT.
- Third-party and regulatory compliance with data privacy, security, access, quality, and ethics drive increased hype to fever pitch.
- Preservation of privacy that may even conflict when operating across multiple jurisdictions.

Obstacles

- Many organizations think that “analytics governance” is different from data and analytics governance, instead of observing the same patterns and solutions that emerge in both.
- Over time, analytics governance will be recognized as part of D&A governance. Hence, stand-alone capabilities will become obsolete before achieving mass-market adoption.
- Vendors who offer analytics, BI, data science and AI solutions are not naturally familiar with or capable of meeting needs of analytic governance. But vendors will often want to meet requests from clients in the positive, so they are trying to develop analytics governance solutions.
- Some solutions that are more capable upstream of data governance in operational use cases are not actually effective at policy execution in analytics use cases. For example, implementing operational MDM in a data lake would create more problems than it might actually solve.

User Recommendations

- Validate your governance charter with the work of policy setting (i.e., governance), policy enforcement (i.e., stewardship) and policy execution (i.e., management) along your analytic pipeline. This will reduce redundancy and save money, and lead to improved outcomes.
- Don’t assume your analytics solutions support your requirements for analytics stewardship (or governance). At most, they might execute a technical rule in their application. You may need to build your own stewardship capability until the vendors meet your needs.
- Don’t assume you need to start with a data or analytics catalog. In case you don’t know your organization’s data and analytics, simply ask your business leaders.

Sample Vendors

Alation; ALTR Solutions; Collibra; ZenOptics

Gartner Recommended Reading

Data and Analytics Leaders Must Use Adaptive Governance to Succeed in Digital Business

Next Best Actions to Improve Your Data and Analytics Governance

Infographic: Data and Analytics Governance Survey: IT Says Mission Accomplished; Business Disagrees

Use Enterprise Metadata Management to Extend Information Governance to Analytics

ModelOps

Analysis By: Joe Antelmi, Erick Brethenoux, Soyeb Barot

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Model operationalization (ModelOps) is primarily focused on the end-to-end governance and life cycle management of advanced analytics, AI and decision models (models based on machine learning [ML], knowledge graphs, rules, optimization, linguistics, agents and others).

Why This Is Important

ModelOps helps companies challenged in standardizing, scaling and augmenting their analytics and AI initiatives that leverage a combination of statistical and ML models. It helps organizations to move their models from the lab environments into production. MLOps primarily focuses on monitoring and governance of ML models, while ModelOps assists in the operationalization and governance of all advanced analytics, decision and AI models (including ML models).

Business Impact

ModelOps delivers business impact in multiple ways. As a practice, it:

- Lays down the foundation for the management of various knowledge representation models, reasoning capabilities and composite model integration.
- Augments the ability to manage decision models and integrate multiple analytics techniques for robust decision making.

- Ensures collaboration among a wider business, development and deployment community, and the ability to correlate analytics and model outcomes with business KPIs.

Drivers

- As the number of advanced analytics, AI and decision models at organizations increase, and as projects become more complicated, organizations will have to manage different types of prepackaged or custom-made models. All will require different operationalization and governance procedures, especially when they are built from scratch.
- Organizations want to be more agile and responsive to changes within their advanced analytics and AI pipelines, not just with models, but also with data, application and infrastructure.
- The operationalization aspects of ML models are not new, but they are in their early stages. However, with ModelOps, the functionalities provided by MLOps are now extended to other non-ML models.
- ModelOps provides a framework to separate responsibilities across various teams for how models (including generative AI, foundational models, analytics, ML, physical, simulation, symbolic, etc.) are built, tested, deployed and monitored across different environments (for example, development, test and production). This enables better productivity and collaboration, and it lowers failure rates.
- There's a need to create resilient and adaptive systems that use a combination of various analytical techniques for decision support, augmentation and automation.
- There is a wide range of risk management concerns across different models — drift, bias, explainability and integrity — that ModelOps helps address.

Obstacles

- Organizations using different types of models in production often don't realize that for some analytics, decision and AI models (rule-based, agent-based, graph, generative AI or simulation models), end-to-end governance and management capabilities can and need to be expanded further.
- Not all analytical techniques currently benefit from mature operationalization methods. Because the spotlight has been on ML techniques, MLOps benefits from a more evolved AI practice, but some models, like agent-based modeling, rule-based models and optimization techniques, require more attention in ModelOps practices and platforms. The creation of applications that leverage generative AI has increased the focus of integrating ModelOps with generative and foundational models, also known as LLMOps in the industry.
- The lack of knowledge relevant to leveraging multiple analytics and AI techniques could prevent organizations from considering the techniques particularly suited to solving specific problems.
- Organizations that are siloed create redundancy in effort with respect to operationalization.

User Recommendations

- Leverage different analytics and AI techniques to increase the success rate of data and analytics initiatives.
- Utilize ModelOps best practices across data, models and applications to ensure transition, reduce friction and increase value generation.
- Extend the skills of ML experts to operationalize a wider range of models. Recruit/upskill additional AI experts to also cover graph analytics, optimization or other required techniques for composite AI
- Establish a culture that encourages collaboration between development and deployment teams, and empowers teams to make decisions to automate, scale and bring stability to the analytics and AI pipeline.
- Collaborate with data management and software engineering teams to scale ModelOps. Offloading operationalization responsibilities to multiple teams enables increased ModelOps specialization and sophistication across the ecosystem of complex AI-enabled applications.
- Optimize the adaptability and efficiency of your AI projects by considering a composite AI approach — integrating various AI techniques to solve business problems.

Sample Vendors

DataRobot; Datatron; IBM; McKinsey & Company (Iguazio); ModelOp; Modzy; SAS; Subex; Valohai; Verta

Gartner Recommended Reading

Top 5 Priorities for Managing AI Risk Within Gartner's MOST Framework

Market Guide for AI Trust, Risk and Security Management

Use Gartner's MLOps Framework to Operationalize Machine Learning Projects

A Mandate for MLOps, ModelOps and DevOps Coordination

Toolkit: Delivery Metrics for DataOps, Self-Service Analytics, ModelOps and MLOps

DevOps Test Data Management

Analysis By: Andrew Bales

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

DevOps test data management is the process of providing DevOps teams with sanitized data to evaluate the performance, functionality and security of applications. It typically includes copying production data, anonymization or masking, and sometimes, virtualization. In some cases, specialized techniques, such as synthetic data generation, are appropriate. Given potential compliance and privacy issues, the efforts frequently involve members of application and data security teams.

Why This Is Important

Test data management is inconsistently adopted across organizations, with many teams still copying production data for use in test environments. As organizations shift to DevOps and the pace of development increases, this traditional approach is increasingly at odds with requirements for efficiency, privacy and security, and even the increased complexity of modern applications. This opens organizations to a variety of legal, security and operational risks.

Business Impact

Quick provisioning of test data helps ensure the pace of development isn't slowed. It's also increasingly important to remain compliant with the growing number of privacy mandates to which organizations are subject. This helps avoid fines and remediation and mitigation costs, along with the inevitable delays associated with audits and investigations. Finally, by providing application teams with anonymized or synthetic data, the risk of data breaches is reduced.

Drivers

- Test data management is generally viewed as a mature, relatively uncomplicated, practice. However, the reality is the combination of the increased pace of development from DevOps and a growing number of privacy mandates and constraints have stressed traditional approaches — prompting the use of virtualization as well as alternative masking and protection techniques, including synthetic data generation.
- More traditional test data management has been inconsistently adopted, with many organizations either simply using copies of production data in unsafe environments or generating “dummy data” (distinct from emerging synthetic data generation techniques) that doesn’t accurately reflect production data. The data privacy requirements and complexity issues noted have prompted organizations to revisit and update their processes with an eye toward scalability and automation. Updated technologies may also be a requirement. For example, requirements for speed and agility have created a need for data virtualization tools.
- Data protection is cited by most Gartner clients in inquiries regarding test data management. Privacy and data protection requirements mean it’s no longer safe to simply provide development teams with a copy of production data since this practice leaves organizations open to increased risk of regulatory violations, data breaches and other security issues.
- With modern applications relying on an increasing number of interconnected data stores (many of which, technologically speaking, are vastly more complex) and applications and APIs to function, testing has become more complex. Such complexity demands that tools support the ability to coordinate and synchronize changes across different data stores to ensure relational consistency while still addressing security and speed mandates.

Obstacles

- In the absence of a strong culture of security, processes and technologies to protect sensitive information during development and testing will encounter friction. Conflicting needs for rapid development and privacy require attention to a mix of organizational and cultural issues to strike a balance across groups.
- Responsibility for test data management in organizations has been shared by application development and database administration. New technologies and processes may shift those responsibilities to include security, complicating organizational dynamics and potentially creating the need for additional resource allocation.
- Implementation can be a burden, especially where little or no data sensitivity classification has been done. This must be accomplished before teams can proceed with the required data transformation and masking. These efforts are typically combined with an analysis of data relationships so that relational integrity can be assured.

User Recommendations

- Involve stakeholders — such as data management, privacy and security teams, compliance teams, etc. — to understand consumption patterns and needs — as appropriate.
- Document existing test data management practices so tools and processes can be evaluated against data protection mandates.
- Coordinate with other teams to avoid duplication of effort and tooling since data masking tools may also be used by analytics teams (e.g., to provide data for machine learning or other purposes).
- Evaluate data masking tooling by considering support for databases and other stores, data discovery capabilities, types of masking supported, and the ability to coordinate change to ensure consistency (e.g., key fields) across multiple sources.
- Evaluate data virtualization for DevOps use cases where frequent updates to test data are required. Virtualization can speed up the process of providing copies of safe data.
- Determine whether synthetic data generation is appropriate in cases where suitable data doesn't exist or reidentification risks are high.

Sample Vendors

BMC Software; Broadcom; DATPROF Delphix; Hazy; Informatica; K2View; Mage; OpenText; Solix Technologies

Gartner Recommended Reading

Market Guide for Data Masking

Elevating Test Data Management for DevOps

3 Steps to Improve Test Data Management for Software Engineering

Innovation Insight for Synthetic Data

Sliding into the Trough

DataOps

Analysis By: Robert Thanaraj, Ehtisham Zaidi, Sharat Menon, Aaron Rosenbaum

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

DataOps is an agile and collaborative data management practice focused on improving the communication, integration, automation, observability and operations of data flows between data engineers and data consumers. The goal is to assist data and analytics (D&A) leaders in driving operational excellence in data delivery in support of their data management solutions.

Why This Is Important

DataOps eliminates various inefficiencies and misalignments between data management and consumption use cases by streamlining data delivery processes and operationalizing data workloads. DataOps practices:

- Improve organizational speed and trust in delivering data
- Manage interdependencies across business processes
- Increase reusability of data engineering work product
- Provide reliable data delivery service levels
- Govern data, leading to trust and use among consumers

Business Impact

- Data engineers benefit from increased productivity and robust change management, ensuring data delivery service levels like quality, lineage and security.
- Data consumers benefit from reduced cycle time of accessing ready-to-use data and improved data trust.

- Organizations thrive on data literacy, productivity gains, self-service enablement and a collaborative culture.
- Eliminate unwanted data delivery efforts by focusing on value flows tied directly to business impact.

Drivers

- Organizations strive to improve speed and efficiency of producing trusted and usable data. DataOps practices reveal bottlenecks in the current D&A delivery process and guide toward improving the lead time (process efficiencies) and cycle time (technical efficiencies).
- DataOps improves the shareability and reusability of the data across the organization. It involves formal processes around data architecture, quality and modeling, and ensures that the data governance requirements are being applied as part of the operational processes. Otherwise, the initial data pipeline would only be designed for a narrow use.
- DataOps practices enable reorganization of teams, which helps overcome the challenges caused by fragmented teams/processes and delays in delivering data in consumable forms.
- DataOps tools eliminate the various inefficiencies and misalignments across data management technologies by streamlining data delivery processes and operationalizing data workloads. It is an emerging technology market.

Obstacles

- Setting up DataOps is a challenge as it needs efforts on justifying operating model shifts, focus on metadata management practices (which are currently nascent) and continuing to provide effort or cost over value justifications which require aligning business outcomes to DataOps activities.
- Organizations have substantial domain expertise and siloed functional capabilities. It is challenging to retain the advantages of the legacy approaches to data management and the people holding those skills, while also aggressively pursuing DataOps.
- Organizations lack a holistic view of various stand-alone technologies that are often managed by multiple teams with varying levels of operational maturity.

- Many strive for end-to-end automation of pipelines driven by code and integrating diverse technologies to make them work together is complex as it involves diverse skill sets.

User Recommendations

- When introducing DataOps, target projects that are struggling due to lack of collaboration, overburdened by the pace of change, or where service tickets from data consumers are piling up.
- Apply the core DevOps approaches to data management such as automating deployment to test environments continuously and managing schema drifts in pipelines. Reach out to your application leaders who have successfully applied DevOps practices to application development.
- Track metrics such as time to deploy changes, degree of automation, developer productivity, code quality, failure rates in production, cost-efficiencies and business impact in dollar amount.
- Plan for data pipeline operations ownership and service-level management. DataOps teams generally own the full development life cycle from inception to production. They must be cross-functional teams that combine data management, software engineering and I&O expertise — some organizations even hire for new roles such as data product manager.

Sample Vendors

Astronomer; BMC; DataKitchen; DataOps.live; GitHub; Kensu; StreamSets; Tengu; Torana (iCEDQ); Unravel

Gartner Recommended Reading

Data and Analytics Essentials: DataOps

Market Guide for DataOps Tools

5 Ways to Enhance Your Data Engineering Practices

How to Apply DevOps and Value Stream Mapping to Data, Analytics and AI

Toolkit: Delivery Metrics for DataOps, Self-Service Analytics, ModelOps and MLOps

Multicloud Management

Analysis By: Lydia Leong

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Multicloud management encompasses the principles, practices and tools necessary to manage multiple cloud infrastructure as a service (IaaS) or platform as a service (PaaS) providers within the context of a multicloud strategy. There are many possible multicloud management approaches, spanning the spectrum from managing each cloud individually to managing all clouds in a unified way.

Why This Is Important

More than 75% of organizations use multiple public cloud IaaS and PaaS providers. Many of these organizations struggle to coordinate governance and management efforts across these multiple providers. Because these providers are highly differentiated from one another, and are often used by different parts of the business for different use cases, it is almost always impractical and inappropriate to apply a “one size fits all” management approach.

Business Impact

Organizations must implement effective cloud management of their public cloud IaaS and PaaS providers to ensure well-governed, safe and efficient cloud adoption that delivers desired business outcomes. Organizations that do not find the right balance between multicloud management consistency and optimal provider-specific management will suffer unnecessarily high multicloud complexity and cost.

Drivers

- All cloud IaaS and PaaS offerings require management, and an organization's efforts to manage cloud providers become more complicated and expensive with every cloud provider added to their portfolio. This has led to a growing interest in effective multicloud management approaches.
- During the early phase of the cloud management platform (CMP) market, vendors sought to promote and sell "single pane of glass" management tools to multicloud customers. While the commercial success of such tools has been limited, the hype has endured.
- More recently, cloud management tool vendors have successfully focused on providing deep, provider-specific support within focused management offerings. However, most such vendors support at least two cloud providers and market multicloud management capabilities.
- Although the "multicloud management" term is broadly hyped, the term is not used consistently across the market. Multicloud management tools may provide visibility or control of cloud resources across one or more capability domains: provisioning and orchestration; service enablement; monitoring and observability; inventory and classification; cost management and resource optimization; cloud migration, backup and disaster recovery; and identity, security, and compliance.
- Although a cloud provider's first-party management services and tools will often meet an organization's management functionality requirements, third-party tools may provide multicloud aggregation, simplification or additional functions not provided by the provider's native capabilities.

Obstacles

- The most effective multicloud strategies result in the use of multiple cloud providers to better exploit the unique capabilities of each provider. Individuals typically only have deep skills with a single provider. This often leads to a desire to optimize the management of each individual provider, rather than a unified multicloud management approach.
- The increased complexity and breadth of cloud services has made it hard or even impossible for a single CMP to meet all the management needs of an organization.
- Each provider has their own strategy for exposing management functionality for their services and different first-party management capabilities. This makes it costly for customers (and cloud management tool vendors) to engineer multicloud management functionality.
- Public cloud IaaS and PaaS offerings have extensive hooks for automated management, but these capabilities vary per service within each provider's portfolio. Service coverage within cloud management tools varies widely.

User Recommendations

- Decide whether you want a single cloud operations function with a unified multicloud approach or a cloud operations approach for each cloud provider. This may lead to different processes, tools and personnel for each major cloud provider you use. You may unify multiple approaches across points of commonality.
- Minimize the number of cloud management tools in use by balancing provider-specific functionality with the desired degree of consistency across your managed environments. This will allow you to contain complexity, cost and the number of vendors to manage, while mitigating the risks associated with them.
- Try not to select a single CMP to manage multiple cloud providers or hybrid clouds. Do not take a "least common denominator" approach that reduces each cloud provider down to only the commoditized capabilities that can be managed through a unified CMP. Organizations that have tried to do so have often failed.

Sample Vendors

CloudBolt Software; Morpheus Data; Scalr; VMware (CloudHealth)

Gartner Recommended Reading

Comparing Cloud Operations Approaches

Quick Answer: How to Navigate Cloud Management Tooling Selection

A Guidance Framework for Selecting Cloud Management Tools

AIOps Platforms

Analysis By: Matt Crossley, Matthew Brisse

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Gartner defines AIOps platform as the application of AI/ML and data analytics at the event management level in order to augment, accelerate and automate manual efforts in the event management process and associated procedures. AIOps platforms are defined by the key characteristics of cross-domain event ingestion, topology assembly, event correlation and reduction, pattern recognition, and remediation augmentation.

Why This Is Important

The combination of increasing application complexity, monitoring tool proliferation, and increasing volumes and varieties of telemetry has shifted complexity from gathering data to interpreting data. AIOps platforms apply machine learning (ML) and data analytics to classify and cluster cross-domain events in near real time, at scale, and in ways that can exceed human capacity. These inferences can augment human analysis, accelerate human response, or automate a process to resolve an issue.

Business Impact

AIOps platforms deliver value through:

- Agility and productivity: By reducing alert fatigue through identification and correlation of related events, operators can focus on fewer, more critical events.
- Service availability and triage cost: By reducing the time and effort required to identify root causes and augmenting, accelerating, or automating remediation.
- Increased value from monitoring tools: By unifying events from siloed tools and learning actionable event patterns across domains.

Drivers

Demand for AIOps platform capabilities is accelerating and is fueled by:

- **Increasing complexity:** Organizations use an increasingly complex mix of IT assets that rely on a highly integrated combination of on-premises assets, cloud IaaS/PaaS providers and SaaS platforms to deliver solutions.
- **Increasing monitoring expectations:** Investments and improvements in monitoring and the pursuit of observability are generating more data from more sources. Increasing demand and advances in monitoring trends, like application performance management (APM) and digital experience monitoring (DEM), present operators with extremely detailed views into their business applications and the end-user experience. Effective use of this additional data requires near-real-time analysis and rationalization of events from related assets and services.
- **Demands for reliability:** Shifts in roles and responsibilities driven by modern operating models, like DevOps and SRE, in the pursuit of greater availability and faster incident resolution. AIOps platforms enable agility by offloading some of the mechanical tasks of event triage, root cause analysis and solution identification. This both accelerates response for common issues and frees up human creative capacity for novel events and business priorities.

Obstacles

- **Unrealistic expectations:** Hype is a major obstacle to AIOps platform adoption. Clients struggle to separate claims of AI and magical automation from achievable use cases. This impacts demonstrating value of AIOps platforms, specifically quantifiable return on investment.
- **Maturity of dependencies:** Benefits of AIOps platforms beyond event correlation requires maturity in dependencies such as automation.
- **Time to value:** AIOps platforms learn through observation, modeling normal data patterns, and associate a solution with these patterns. This can take time depending on the frequency of occurrence. Developing accurate detection models for rare events can take months.
- **Market shifts and maturity:** Monitoring vendors are moving up the stack, AIOps platform vendors are reaching into monitoring domains, and ITSM vendors use AIOps capabilities to extend their reach. Expect further convergence and market shifts to change the definition of “state of the art.”

User Recommendations

- Establish clear, realistic use cases for an AIOps platform pilot and validate them individually, rather than all at once. This approach helps reveal pockets of potential value that might be missed when evaluating only the aggregate impact. Ultimately, this fundamental step underpins an eventual strategy, while scoping the vendor landscape, clarifying technical and process dependencies, and separating hype from reality.
- Layer the AIOps features within monitoring tools with the cross-domain analysis of an AIOps platform. This approach enables efficient data ingestion and analysis, and the surfacing of insights across domains.
- Do not require automation outcomes for all AIOps applications. There is tremendous value in accelerating and augmenting human activity. These approaches often avoid the challenge of the probabilistic uncertainty combined with automated change in production environments.

Sample Vendors

BigPanda; BMC Software; Digitate; IBM; Interlink; Moogsoft; OpsRamp; PagerDuty; ServiceNow; Splunk

Gartner Recommended Reading

Market Guide for AIOps Platforms

Deliver Value to Succeed in Implementing AIOps Platforms

Infographic: Artificial Intelligence Use-Case Prism for AIOps

Infographic: AIOps Architecture for Analyzing Operational Telemetry

How Do I Plan for Migrating My Data Center Infrastructure Into an XaaS Model?

Infrastructure Automation

Analysis By: Chris Saunderson

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Infrastructure automation (IA) enables DevOps and infrastructure and operations (I&O) teams to deliver automated infrastructure services across on-premises and cloud environments. This includes the life cycle of services through creation, configuration, operation and retirement. These infrastructure services are then made available through platform delivery, self-service catalogs, direct invocation and API integrations.

Why This Is Important

IA delivers velocity, quality, efficiency and reliability, with scalable, declarative approaches for deploying and managing infrastructure. These tools integrate into delivery pipelines targeting deployment topologies that range from on-premises to the cloud, and enable infrastructure consumers to build what is needed when they need it. Once deployed, IA provides day-2 and beyond operational automation, and extends to provide policy compliance and enforcement capabilities.

Business Impact

Implementing and maturing IA services will enable:

- **Agility** — continuous infrastructure delivery and operations
- **Productivity** — version-controlled, declarative, repeatable, efficient deployments
- **Cost improvement** — reductions in manual effort expended via increased automation
- **Risk mitigation** — compliance driven by standardized configurations
- **Collaboration** — delivering environments that product teams need with security, cost and compliance requirements baked in.

Drivers

I&O leaders must automate delivery through tool and skills investments to mature beyond simple deployments. The target should be standardized platforms that deliver the systemic, transparent management of platform deployments. This same discipline must be applied to the operation of these deployed platforms, ensuring that efficient operations (including automated incident response) can be achieved. IA tools deliver the following key capabilities to support this maturation:

- Multicloud/hybrid cloud infrastructure delivery
- Support for immutable and programmable infrastructures
- Predictable delivery enabling automated operations
- Self-service and on-demand environment creation
- Integration into DevOps initiatives (continuous integration/delivery/deployment)
- Resource provisioning, including cost optimization capabilities
- Operational configuration management efficiencies
- Policy-based delivery and assessment/enforcement of deployments against internal and external policy requirements
- Enterprise-level framework to enable maturing of automation strategies
- Skills and practice development inside infrastructure teams, enabling agile and iterative development and sustaining of services

Obstacles

- The combination of tools needed to deliver IA capability can increase tool count and complexity.
- Software engineering skills and practices are required to get maximum value from tool investments.
- IA vendor capability expansion overlaps and confuses the tool landscape, resulting in over-investment.
- Steep learning curves can cause developers and administrators to revert to familiar scripting methods to deliver required capabilities.

User Recommendations

- Identify existing IA tools in use to catalog capabilities, identify use cases and document overlaps to aid decision making.
- Assess existing internal IT skills to incorporate training needs that more fully enable IA, especially for an automation architect role to coordinate standards development and implementation.
- Baseline how managed systems and tooling will be consumed (e.g., engineer, self-service catalog, API or on-demand).
- Integrate security and compliance requirements into scope for automation and delivery activities.
- Develop an IA tooling strategy that incorporates current needs and near-term roadmap evolution.

Sample Vendors

Amazon Web Services; HashiCorp; Microsoft; Perforce; Pliant; Progress; Pulumi; RackN; Upbound; VMware

Gartner Recommended Reading

Market Guide for Infrastructure Automation Tools

Innovation Insight for Continuous Infrastructure Automation

To Automate Your Automation, Apply Agile and DevOps Practices to Infrastructure and Operations

How to Start and Scale Your Platform Engineering Team

Product-Centric Delivery Model

Analysis By: Mike West, Sarah Davies

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

A product-centric delivery model allows you to take advantage of product management. That is to structure your organization's operating model to create small teams focused on product development and provide greater flexibility to meet the shifting demands of consumers. This allows organizations to adapt how software is consumed, and enables software leaders to shift from time-bound episodic delivery to continuous delivery.

Why This Is Important

The ability to respond to market trends, the economy and shifting consumer demands without complex organizational changes is driving organizations to adopt the product-centric delivery model. This model allows organizations to have greater control of their enterprise strategy and move away from the standard, functional skill-based organization and embrace multiskilled persistent teams that work together on a product or product line.

Business Impact

A product-centric delivery model enables an enterprise to:

- Focus on outcomes rather than functions, and incremental improvements to measured business outcomes.
- Use venture capital or investment funding models as financial methods to control investment at operational levels.
- Improve agility to respond to changing market demands and customer value prioritization.
- Reduce silos, improve collaboration across product value streams, and have flatter organization and more rapid decision making.

Drivers

- Organizations must adjust their delivery models to keep pace with market demands and increased volatility.
- Investment and financial models need to provide flexibility and support evidence-based market research and responses to corporate strategy.
- Organizations need rapid, incremental feedback that engineering teams can respond to flexibly to satisfy and delight customers.
- A shift to cloud-based architecture is driving the adoption of value-based operating models that reflect the customer journey rather than existing management frameworks.
- The continuous disbanding of project teams has left today's organizations feeling the need to address new talent retention strategies and to overcome inefficiencies caused by siloed data and solutions via continuous innovation and delivery.

Obstacles

The key factors hampering the adoption of product-centric delivery models include:

- Inertia from existing organizational culture and management frameworks reluctant to disband current budgets and authority positions. This is compounded by the difficulty finding experienced product management subject matter experts, e.g., product managers, to help overcome this reluctancy.
- Walls between business and IT due to the lack of alignment around outcomes, responsibilities, siloed budgets and success metrics, which leads to a lack of understanding of business outcome metrics such as leading key performance indicators (KPIs) and objective and key results (OKRs).
- The lack of senior management and organizational support, which leaves adoption in pockets across the organization, and outmoded governance processes incentivizing control and risk aversion rather than experimentation and innovation.

User Recommendations

- Establish clear goals and objectives for the transition, anchored on business priorities, building leadership support for the necessary culture and governance change.
- Establish a strong partnership with colleagues as you identify and train product managers, product owners, business leaders and team members on agile and product management practices.
- Transform governance to embrace business architecture practices such as value stream mapping, business capability modeling, and customer and employee journey mapping.
- Move to a product funding and work prioritization model that allows for reallocation of resources based on business demand and changing market conditions. Create an explicit network of dashboards to convey the outcomes of product initiatives. Manage recurring reviews of outcomes to assess the value of work underway.

Gartner Recommended Reading

Strengthen Five Key Pillars of Product Management to Scale for Digital Business Success

Prepare Now for the Future of Digital Product Management

Improve Product Team Speed and Agility by Minimizing Dependencies: Approaches From 3 Leading Organizations

Overcome Objections and Sell the Benefits of Moving From Projects to Products and Agile

Create a Product Operations Role to Improve the Strategic Focus of Product Managers

CloudOps

Analysis By: Miguel Angel Borrega, Philip Dawson, Lydia Leong

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Adolescent

Definition:

CloudOps is short for “cloud operations,” and is the set of practices and processes used to manage and support an organization’s consumption of public cloud infrastructure as a service (IaaS), platform as a service (PaaS) and SaaS. CloudOps encompasses cloud administration, operations and engineering, but is distinct from cloud governance.

Why This Is Important

Public cloud IaaS, PaaS and SaaS are all shared-responsibility models. Organizations that consume cloud services must understand their responsibilities for each service they consume. IT organizations are often responsible for fulfilling these responsibilities. However, cloud operations models are evolving as service consumers outside of the central I&O team (such as developers, data scientists or business users) increasingly assume some or most such responsibilities.

Business Impact

Organizations must find the appropriate balance between enabling improved business agility through cloud adoption, and ensuring that cloud services are used safely and efficiently. Cloud operations models are not “one size fits all.” The allocation of responsibilities and the processes used will determine the roles and skills necessary. The greater the delta between the cloud operations model and the on-premises operations model, the more transformation will be necessary.

Drivers

- Organizations need to formalize their cloud operations model. Many of them begin cloud adoption with an ad hoc operations model in which individuals contribute to a cloud project as necessary — and on a temporary basis. However, as the number of projects and the level of effort rise, a more formal operations approach becomes necessary.
- An organization's selection of a cloud operations approach is usually primarily driven by its choice of cloud management style for IaaS and PaaS. While SaaS still requires some governance and management, IaaS and PaaS demand constant operations, engineering and security efforts.
- Organizations with a lack of internal cloud skills can hardly manage their cloud platform efficiently and require the help of cloud managed service providers (MSP) to deliver a reliable cloud operations model. MSPs can offer cloud operations in a variety of styles.
- A DevOps-centric cloud operations model enables cloud native developments on IaaS and PaaS. Many organizations explicitly choose to embrace this model to increase their business agility and to accelerate their modernization initiatives.
- The drive toward cloud-enabled self-service (for application developers, data scientists and other technical end users) often causes organizations to rethink their operations model for the cloud. Some organizations desire to adopt a "You Build It, You Run It" model which makes application teams accept principal responsibility for production operations of their applications, rather than relying primarily on the I&O team. However, this approach requires strong platform engineering support to avoid placing the burdens of excessive cognitive load and unnecessary toil on cloud consumers.

Obstacles

- Many organizations lack the skills necessary to effectively manage cloud environments. Consequently, they attempt ad hoc cloud operations approaches to “make do” as best they can. Such approaches result in unmanaged risks, the steady accumulation of unknown levels of technical debt and unnecessarily high cloud costs.
- Organizations that conduct lift-and-shift migrations to cloud IaaS often adopt a hybrid management style where cloud management is performed almost identically to on-premises management, but this is suboptimal and usually only viable as a short-term approach.
- Many organizations do not plan their transition to a long-term cloud operations model. This leaves them unprepared for the transformation in roles, skills and mindsets necessary to maximize the business and technical benefits of cloud computing.

User Recommendations

- Establish a formal cloud operations approach as soon as the organization has moved beyond an initial public cloud adoption to have an optimal cloud journey.
- Source a capable cloud MSP if necessary to facilitate the transition to a new operations approach.
- If you are currently outsourcing your infrastructure operations, do not expect your existing outsourcing team to successfully transform. You must replace the team — and may need to switch outsourcers.
- Avoid embedding cloud operations functions within the technology-oriented I&O organization focused on on-premises management.
- Base your cloud operations model decisions on these key factors: business requirements, cloud focus, automation emphasis, developer independence, service models adopted (IaaS, PaaS, SaaS) and suitability for multicloud.
- Organizations operating under a CloudOps approach could evolve to cloud platform ops or platform engineering models, implementing cloud-native design patterns and DevOps automation.

Gartner Recommended Reading

Comparing Cloud Operations Approaches

Guidance Framework for Implementing Cloud Platform Operations

Cloud-Native Requires New Thinking for Cloud Operations Service Providers

Tool: Cloud Operations — Capability Examples and Planning Hot Topics

Climbing the Slope

Cloud Center of Excellence

Analysis By: Lydia Leong

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition:

A cloud center of excellence (CCOE) is a centralized enterprise architecture function that leads and governs cloud computing adoption within an organization. Its role is to enable and empower the organization on its cloud journey, not to execute cloud implementation itself.

Why This Is Important

A CCOE is an effective way to drive enterprise-scale cloud adoption that results in positive business outcomes. As an enterprise architecture (EA) function, it leads organizationwide cloud governance and brokerage, and guides cloud transformation. Although the CCOE is responsible for developing cloud computing policies, it primarily influences, rather than controlling. It enables and empowers the teams that are implementing the cloud journey with the guidance they need for successful execution.

Business Impact

The CCOE drives strategic cloud adoption through three core functions — cloud brokerage, cloud governance and cloud transformation. It serves as an internal cloud consulting practice that delivers cloud architectures and recommended solutions. It partners with the sourcing team to provide cloud vendor management, including cloud cost governance. It raises the organization's level of cloud expertise and supports transformation efforts through its leadership of a cloud community of practice.

Drivers

- The impetus to form a CCOE generally comes from the realization that the organization needs to mature or scale its cloud adoption, or to ensure that cloud computing delivers desired business benefits. Specifically, the organization needs to ensure that the "path of least resistance" for cloud use is also the path that is well governed and meets the organization's security and regulatory compliance requirements.
- An organization needs a guide on its cloud journey, as cloud use grows within the organization and the organization discovers the best practices for cloud usage that are specific to its business needs. The CCOE, governance guidelines and guardrails, and solutions must evolve with the business and its cloud use.
- Many businesses need help with cloud-enabled digital transformation, ideation of new cloud-enabled business innovations and "evangelism" to encourage cloud adoption.
- The creation of a CCOE is strongly encouraged by many cloud providers, as well as cloud managed service providers (MSPs). However, cloud providers often encourage the creation of vendor-specific CCOEs, rather than broad CCOEs that cut across IaaS, PaaS and SaaS lines. MSPs often promote CCOEs because they tend to result in significant managed or professional services revenue.
- Some organizations initially adopt a cloud operating model that uses a consolidated cloud competence center team that blends all functions necessary for cloud implementation. Such organizations often discover that they need to separate cloud governance and other cloud enterprise architecture capabilities from cloud implementation.

Obstacles

- The CCOE needs the sponsorship and mandate of the CIO or another C-level executive to be effective.
- Many organizations make mistakes in setting the structure and mission of the CCOE, resulting in a failure of the CCOE to make the desired business impact. The CCOE is fundamentally a business-outcome-driven enterprise architecture function, not a sourcing or infrastructure and operations function.
- The CCOE is typically small, and its effectiveness depends on educating and influencing others throughout the organization who are actually implementing the use of cloud services.

- Staffing the CCOE is often challenging, even though it is typically small. There is significant labor market competition for this skill set, and it may, therefore, be necessary to open headcount for cloud architects well in advance of demand. Understaffing the CCOE can be a major threat to its influence and success. However, the CCOE should not be fully outsourced, due to its strategic nature.

User Recommendations

- A CCOE is an EA function that should be led by a chief cloud architect and staffed by cloud architects. Some organizations hire an individual contractor with very strong knowledge of their primary cloud services to lead their CCOE, but such an individual needs an enterprise architect partner with very strong knowledge of the business and the necessary cross-functional relationships. In most cases, these are full-time, senior-level, individual-contributor roles.
- The chief cloud architect should also lead a cross-functional cloud computing advisory committee that contains representatives from the business; technical end-user teams (such as the application development teams); infrastructure and operations; and sourcing, security, compliance, risk management and legal teams. This committee is primarily concerned with strategy and policy.
- Neither the committee nor the CCOE should be a cloud implementation function. That role is typically occupied by a cloud operations function.

Gartner Recommended Reading

How to Deploy a Cloud Center of Excellence

Infographic: Gartner's Reference Cloud Operating Model

How to Design a Cloud Operating Model and Build a Cloud Center of Excellence

Solution Path for Implementing a Cloud Center of Excellence

Innovation Insight for the Cloud Center of Excellence

Entering the Plateau

DevSecOps

Analysis By: Neil MacDonald, Mark Horvath

Benefit Rating: Transformational

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

DevSecOps is the integration and automation of security and compliance testing into agile IT and DevOps development pipelines, as seamlessly and transparently as possible, without reducing the agility or speed of developers or requiring them to leave their development toolchain. Ideally, offerings provide security visibility and protection at runtime as well.

Why This Is Important

DevSecOps offers a means of effectively integrating security into the development process, in a way that eliminates or reduces friction between security and development. The goal is to pragmatically achieve a secure, workable software development life cycle (SDLC) supporting rapid development. DevSecOps has become a mainstream development practice, although the specifics can vary between organizations based on their technology and the maturity of their development processes.

Business Impact

The goal of DevSecOps is to speed up development without compromising on security and compliance. Furthermore, the externalization of security policy enables business units and security organizations to define and prioritize policy guardrails and lets developers focus on application functionalities. Policy-driven automation of security infrastructure improves compliance, the quality of security enforcement and developer efficiency, as well as overall IT effectiveness.

Drivers

- Adoption of DevOps, and other rapid development practices, requires security and compliance testing that can keep up with the rapid pace of development.

- DevSecOps offerings are applied as early as possible in the development process, whereas traditional application security testing (AST) tools associated with older development models are applied late in the development cycle, frustrating developers and business stakeholders.
- Testing results need to be integrated into the development process in ways that complement developers' existing workflows and toolsets, and not require them to learn skills unrelated to their goals.
- The use of open source has greatly increased the risk of the inadvertent use of known vulnerable components and frameworks by developers.

Obstacles

- Incorrectly implemented, siloed and cumbersome security testing is the antithesis of DevOps. Due to this, developers believe security testing tools are slowing them down.
- Developers don't understand the vulnerabilities their coding introduces.
- Developers don't want to leave their development (continuous integration/continuous delivery [CI/CD]) pipeline to perform tests or to view the results of security and compliance testing tools.
- Historically, static application security testing (SAST) and dynamic application security testing (DAST) tools have been plagued with false positives or vague information, hence frustrating developers.
- The diversity of developer tools used in a modern CI/CD pipeline will complicate the seamless integration of DevSecOps offerings.

User Recommendations

- "Shift left" and make security testing tools and processes available earlier in the development process.
- Prioritize the identification of open-source software (OSS) components and vulnerabilities in development (referred to as software composition analysis).
- Opt for automated tools with fast turnaround times, with a goal of reducing false positives and focusing developers on the highest-confidence and most-critical vulnerabilities first.

- Ask vendors to support out-of-the-box integration with common development tools and support full API enablement of their offerings for automation.
- Evaluate emerging cloud native application protection platform (CNAPP) offerings for technical control implementation.
- Require security controls to understand and apply security policies in container- and Kubernetes-based environments.
- Favor offerings that can link scanning in development to correct configuration, visibility and protection at runtime.

Sample Vendors

Apiiro; Aqua Security; Contrast Security; Dazz; Lacework; Palo Alto Networks; Qwiet AI; Snyk; Sonatype; Wiz

Gartner Recommended Reading

How to Select DevSecOps Tools for Secure Software Delivery

Market Guide for Cloud-Native Application Protection Platforms

Magic Quadrant for Application Security Testing

12 Things to Get Right for Successful DevSecOps

How to Manage Open-Source Software Risks Using Software Composition Analysis

Appendixes

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Source: Gartner (July 2023)

Table 3: Benefit Ratings

Benefit Rating ↓	*Definition* ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2023)

Table 4: Maturity Levels

(Enlarged table in Appendix)

Maturity Levels ↓	*Status* ↓	*Products/Vendors* ↓
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2023)

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner's Hype Cycles

Tool: Create Your Own Hype Cycle With Gartner's Hype Cycle Builder

Executive Essentials: Compose Your IT Operating Model to Generate Value

Redesign the IT Operating Model to Accelerate Digital Business

Infographic: Artificial Intelligence Use-Case Prism for AIOps

How to Design a Cloud Operating Model and Build a Cloud Center of Excellence

Top Strategic Technology Trends for 2023: Platform Engineering

Sustainability: A Customer Priority and Provider Imperative

Table 1: Priority Matrix for Operating Models, 2023

Benefit ↓	*Years to Mainstream Adoption*			
	Less Than 2 Years ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
Transformational	DevSecOps	NetDevOps Platform Engineering	Augmented FinOps Platform Operating Model	
High	Cloud Center of Excellence Product-Centric Delivery Model	Cloud Resilience Cloud Sustainability DataOps FinOps GitOps Infrastructure Automation Infrastructure Orchestration	AIOps Platforms DesignOps Infrastructure Platform Engineering ModelOps Operational AI Systems	YBI YRI
Moderate		CloudOps DevOps Test Data Management Multicloud Management	GreenOps	
Low				

Source: Gartner (July 2023)

Table 2: Hype Cycle Phases

Phase	*Definition*
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Phase ↓	Definition ↓

Source: Gartner (July 2023)

Table 3: Benefit Ratings

Benefit Rating ↓	Definition ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2023)

Table 4: Maturity Levels

Maturity Levels ↓	*Status* ↓	*Products/Vendors* ↓
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2023)