Gartner®

Hype Cycle for I&O Automation, 2023

Published 14 July 2023 - ID G00788741 - 141 min read

By Analyst(s): Chris Saunderson, Cameron Haight

Initiatives: I&O Operations Management

Automation is key to transforming the capabilities that infrastructure and operations teams deliver as organizations pursue greater value, agility and efficiency. This Hype Cycle will help I&O leaders looking to deliver efficiencies and innovations, upskill staff, and optimize costs and value.

Additional Perspectives

- Summary Translation: Hype Cycle for I&O Automation, 2023 (28 August 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

Strategic Planning Assumptions

By 2025, 70% of organizations will implement structured infrastructure automation to deliver flexibility and efficiency, which is a significant increase from 20% in 2021.

By 2026, 50% of enterprises will use artificial intelligence (AI) functions to automate Day 2 network operations, compared with fewer than 10% in 2023.

By 2027, 75% of enterprises will use site reliability engineering practices organizationwide to optimize product design, cost and operations to meet customer expectations, up from 10% in 2022.

By 2025, 70% of organizations will complement continuous delivery of applications with continuous infrastructure automation to improve business agility, which is a significant increase from fewer than 20% in 2021.

By 2025, 30% of enterprises will have implemented artificial intelligence (AI)-augmented development and testing strategies, which is a major increase from 5% in 2021.

By 2025, 25% of enterprises will automate more than half of their network activities, an increase from fewer than 8% of enterprises in early 2022.

By 2025, 40% of organizations will implement chaos engineering practices as part of site reliability engineering (SRE) initiatives, improving mean time to repair (MTTR) by 90% on average.

Analysis

What You Need to Know

Automation is a transformational investment for infrastructure and operations (I&O) leaders. Investments in this area reflect the need to enable improved speed to market, increased business agility, mitigation of security and compliance risk, optimization of performance, and minimization of service costs.

Recent rapid advances in generative artificial intelligence (GenAI) offer efficiency gains to organizations building and sustaining automation. Code-writing assistants can now help with the initial development of automation templates, playbooks, rules and other artifacts.

Automation profoundly affects the roles, skills and expectations of I&O leaders and their staff. It is a means by which staff engagement, knowledge and experience can be improved.

This Hype Cycle offers insight into technologies pivotal to success with I&O automation.

I&O leaders responsible for automation must:

- Create a service-oriented automation strategy based on delivering a “platform as a product” (see How to Start and Scale Your Platform Engineering Team).
- Increase agile skills in I&O teams to drive continuous delivery improvement (see Case Study: Installing Agile Ways of Working in Infrastructure (Audi)).
- Explore generative AI for I&O automation use cases (see Quick Answer: What 3 Actions Should I&O Leaders Take Now on ChatGPT?).
- Adopt a use-case-driven approach to intelligent automation (IA) tools and AI for IT operations (AIOps) platforms and domain-centric tools (see Monitoring and Observability for Modern Infrastructure and Applications).
- Expand automated pipelines to deliver infrastructure services (see Case Study: Infrastructure Platform Teams for Self-Service Delivery (Politiet)).

For more information about how I&O leaders view technologies aligned with this Hype Cycle, see Infographic: 2023 Technology Adoption Roadmap for Infrastructure and Operations.

The Hype Cycle

Automation is the engine that accelerates delivery of value. I&O leaders must view automation as a core capability that optimizes performance and enables velocity and efficiency as they embrace the overarching trends of programmable infrastructure, hybrid infrastructure and platform approaches to operations.

Four factors are behind the rise of I&O automation technologies:

- **Business requirements:** Delivering new and expanded business capabilities, while optimizing performance and driving efficiency in operating foundational platforms, is impossible without automation. The role of “developer” has expanded to include I&O, and it enables emerging roles such as infrastructure platform engineer and reliability engineer.
- **Infrastructure scale:** Broadened service topologies, extending beyond on-premises and cloud deployments to the edge, colocation and Internet of Things (IoT) spheres, challenge conventional approaches and enable efficient delivery and operational governance.
- **Software engineering:** Platform engineering is being adopted as a centralized approach to the delivery and support of critical applications, and enabling organizations to satisfy security, compliance and cost imperatives in relation to their infrastructure products.
- **Environment complexity:** As AI capabilities keep evolving, AIOps, GenAI and I&O automation are combining to extend capabilities beyond issue identification and remediation. Augmented and autonomous responses continue to be implemented.

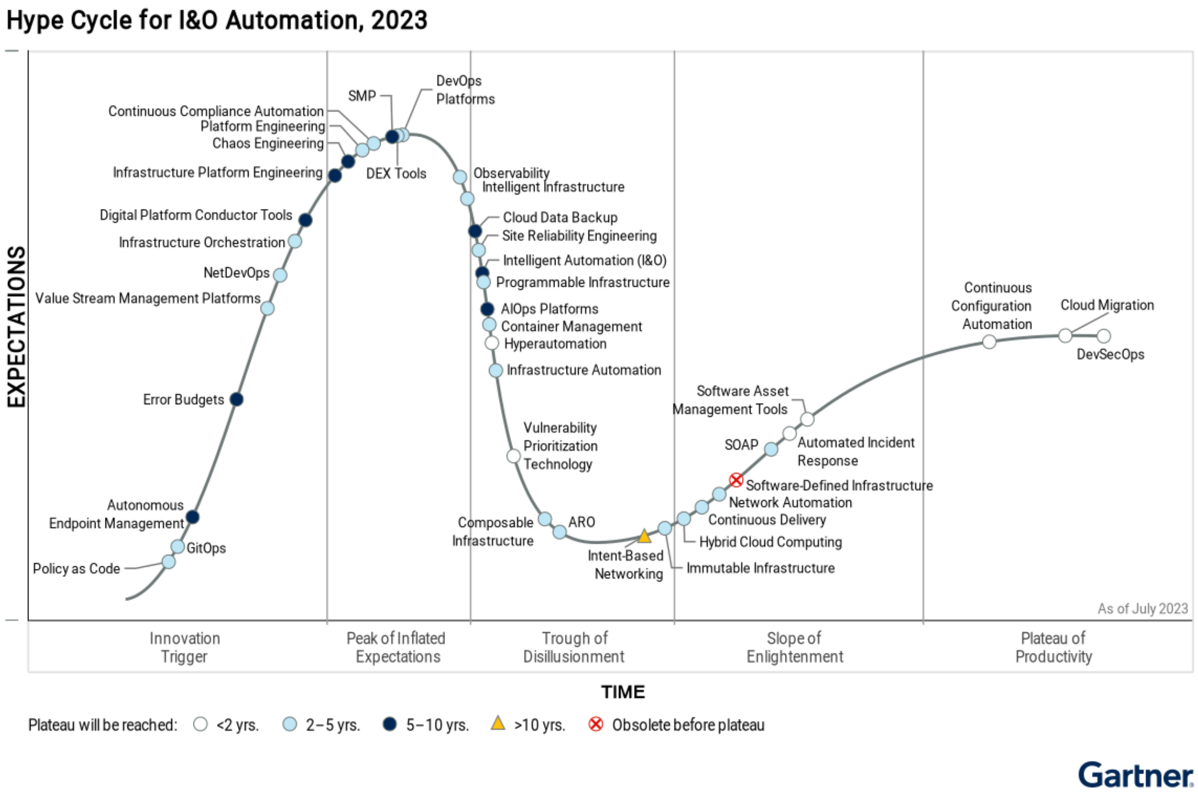
Service orchestration and automation tools remain foundational to delivering reliability, efficiency and productivity returns. Vendors have modernized these tools to integrate AI and machine learning techniques, include broader technology integrations, and support agile delivery to improve the scope and quality of automation. Efforts to combine automation technologies in order to extend I&O’s contribution to hyperautomation initiatives continue and are extending the value of I&O automation to business-centric domains.

Workload deployment patterns that are expanding to include on-premises, colocation, edge, cloud and IoT targets continue to stretch I&O teams' ability to manage broader platforms that support workload delivery. The proliferation of composable and programmable infrastructures that embed an API-driven approach to managing infrastructure increases the pressure for I&O teams to have software engineering skills to support initiatives in this area. I&O leaders need to develop or acquire these skills in a competitive market and explore how the use of GenAI could enhance skills development and efficient automation development.

Platform teams continue to gain traction among Gartner clients. They represent an "automation first" approach to delivery, embedding agile methods of working and DevOps practices to improve capability, efficiency, customer centricity and innovation in application delivery in order to make transformation efforts successful and sustainable.

Organizations are using AI more broadly to detect and resolve problems sourced from both users and observability platforms, and are enabling rapid feedback loops to drive operational and reliability improvements. Insight generation and action recommendations are improving the responsiveness of service operations and helping teams learn and improve iteratively.

Figure 1: Hype Cycle for I&O Automation, 2023



The Priority Matrix

The Priority Matrix maps the time it is likely to take for Hype Cycle entries to achieve mainstream adoption against the level of benefit they are likely to provide. It therefore helps answer two important questions:

1. How much value will an organization derive from an innovation?

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

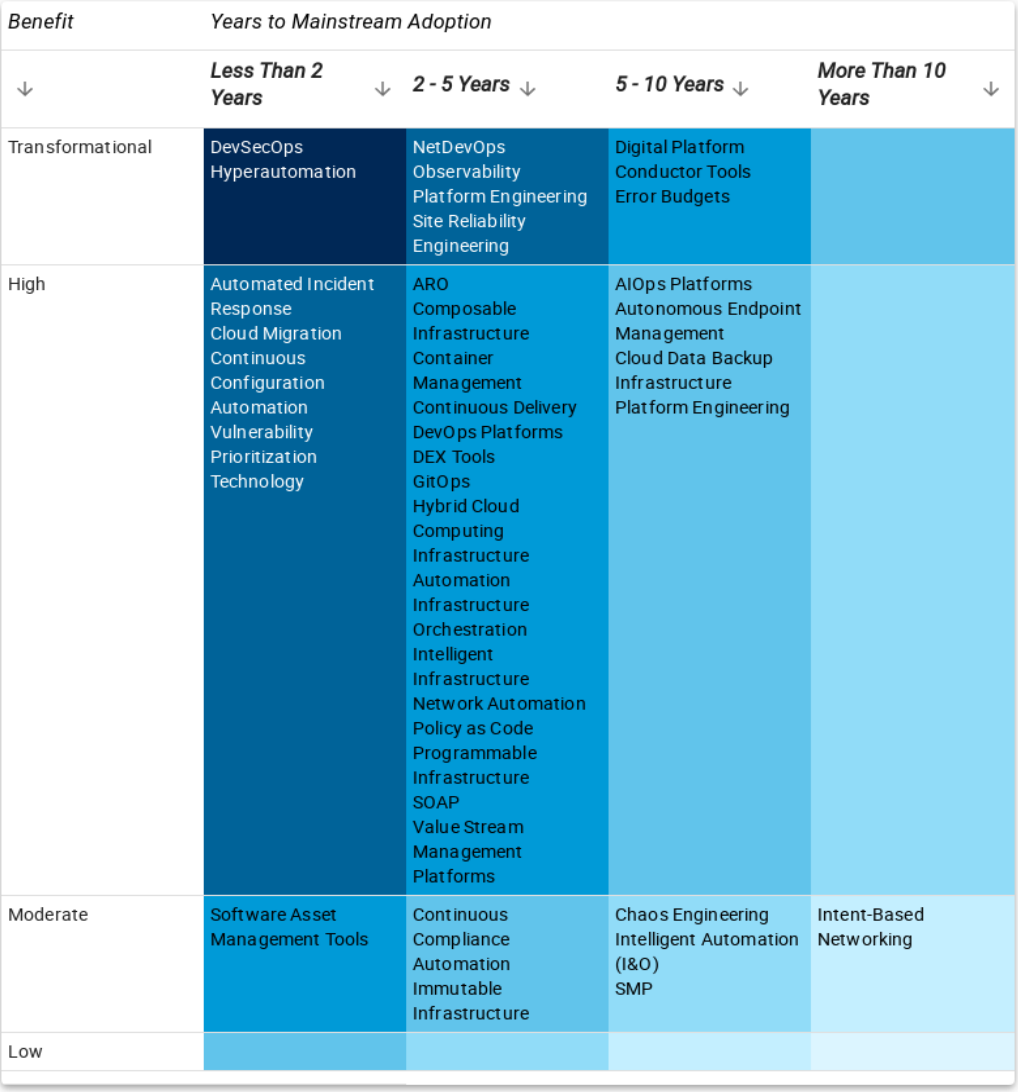
During the next two to five years, infrastructure platform engineering, GenAI and delivery demands will drive automation investments. I&O leaders must scale their provisioning and management approaches beyond their data centers and traditional cloud presences, and include the edge and the IoT in their topologies. DevOps platforms, infrastructure orchestration and infrastructure automation technologies form the core of the automation that I&O teams will support and use themselves, supplemented by GenAI capabilities. Adjacent disciplines, such as site reliability engineering (SRE), chaos engineering and infrastructure cost optimization will become integral to efforts to support modern service delivery. Digital platform conductor tools will maximize the use of high-cost components, and drive intelligent workload orchestration on-premises, at the edge and in the cloud. Workload placement and optimization strategies, enabled by automation, will become even more important as the evaluation and reevaluation of workload locations, in light of business and technical constraints, matures.

Infrastructure automation and infrastructure orchestration enhance application delivery and support the widening of deployment targets. GitOps and policy-as-code approaches and tools, supplemented by vulnerability prioritization technology platforms, will drive assessment and enforcement of security and compliance mandates. Similarly, adoption of chaos engineering and SRE approaches will improve the resilience and availability of delivered platforms.

Increased use of AI techniques across the technology spectrum enables I&O teams to improve decision-making speed, automation development efficiency and the accuracy of actions. Future IT operations automation will be more autonomous, and will need IA tools to deliver higher-value business services.

Table 1: Priority Matrix for I&O Automation, 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 Hyperautomation	NetDevOps Observability Platform Engineering Site Reliability Engineering	Digital Platform Conductor Tools Error Budgets	
High	Automated Incident Response Cloud Migration Continuous Configuration Automation Vulnerability Prioritization Technology	ARO Composable Infrastructure Container Management Continuous Delivery DevOps Platforms DEX Tools GitOps Hybrid Cloud Computing Infrastructure Automation Infrastructure Orchestration Intelligent Infrastructure Network Automation Policy as Code Programmable Infrastructure SOAP Value Stream Management Platforms	AIOps Platforms Autonomous Endpoint Management Cloud Data Backup Infrastructure Platform Engineering	
Moderate	Software Asset Management Tools	Continuous Compliance Automation Immutable Infrastructure	Chaos Engineering Intelligent Automation (I&O) SMP	Intent-Based Networking
Low				

Source: Gartner (July 2023)

Off the Hype Cycle

- Value stream delivery platforms have matured into DevOps platforms. They remain critical I&O investments for developing the practices and capabilities needed to make full use of tools that increase efficiency and innovation.

- Hybrid digital infrastructure management (HDIM) has been incorporated into digital platform conductor tools.

- ITIL, as both a practice and an implementation, has matured to the extent that it no longer appears on the Hype Cycle.

- Cloud management platforms have matured into the cloud management tools market.

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

Policy as Code

Analysis By: Paul Delory

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Policy as code (PaC) languages express governance and compliance rules as code, so they can be enforced programmatically by automation tools. PaC languages are often domain-specific and declarative. With PaC, policies are treated as software, making them subject to version control, code review and functional testing. The most mature PaC tools can render any business logic in code. You can use them today to enforce infrastructure compliance, authorization, Kubernetes admission control, and more.

Why This Is Important

In the most mature automation pipelines, infrastructure and operations (I&O) engineers mostly spend time on optimization, governance and compliance. They no longer build infrastructure; that work has been automated and turned over to others. Now, the I&O function builds the guardrails around the infrastructure services that their end users consume. I&O must align with security and compliance teams. PaC brings policy enforcement into their automation pipelines, while preserving a separation of duties that mirrors a typical IT org chart.

Business Impact

Policy as code improves:

- **Security, compliance and automation:** PaC combined with infrastructure automation implements policies automatically, with implicit compliance guarantees.
- **Alignment of security and operations teams:** PaC allows security and compliance teams to interface directly with automation pipelines to ensure conformance.
- **Visibility and auditability:** PaC provides both documentation of policies and evidence they are being enforced.
- **Time and effort spent:** PaC means less toil for operators.

Drivers

- **PaC tooling:** Several dedicated PaC tools are now on the market, many of them are open-source. The Open Policy Agent, a Cloud Native Computing Foundation project, has become the *de facto* standard for PaC. Indeed, even some other PaC tools now use Open Policy Agent policies alongside or instead of their own policy engines.
- **Increasing regulation:** New regulations such as GDPR have increased both the difficulty of compliance and the pressure on compliance teams. PaC allows compliance teams and auditors to document their policies in detail, and to verify that they are being enforced.
- **Security breaches:** Similarly, a spate of newsworthy security breaches at public companies — caused by infrastructure misconfigurations — has put every IT organization's security and compliance practices under increased scrutiny. No I&O team wants its security failures to be the reason for its company getting negative headlines.
- **Growth of DevOps and DevSecOps:** More and more companies are embracing DevOps and DevSecOps — which means more and more companies are encountering the hard governance problems of automation. Many teams that implement infrastructure as code quickly are finding that they need better policy enforcement, and PaC can help.
- **Cloud optimization and cost control:** Beside their benefits for security and compliance, PaC tools can also be used to enforce the build standards for infrastructure, including budgets. In the public cloud, where oversized or unnecessary infrastructure incurs direct out-of-pocket costs, programmatically enforced policies can help to control spending.

Obstacles

- **Scarcity of downloadable content:** PaC tools will not gain real traction until they have an extensive library of community-generated content. Ideally, users would simply download the policies they need from a free, public repository, rather than having to write their own policies. Over time, as the user base expands and commercial offerings see increased adoption, PaC tools will reach a critical mass of downloadable content that supports real-world use cases.

- **Skill set:** Many I&O professionals lack the skills to operate automation and PaC tools effectively. Gartner clients routinely report that their automation and policy management are hindered primarily by people, not tools. PaC will magnify these existing skills challenges.

- **Organizational inertia:** PaC promises improved collaboration between I&O and security or compliance teams. But in some organizations, this change would be unwanted. Internal resistance of this kind will slow the rate, scope and scale of PaC initiatives.

User Recommendations

- **Start small:** Choose a pilot use case where PaC is likely to provide real business benefits, expanding to others once PaC has proven its value.

- **Upskill staff:** PaC languages are not always intuitive. Technical staff will need practice to reach proficiency.

- **Prioritize existing templates:** Focus your PaC efforts on use cases that have ready-made implementation templates — ideally, publicly available downloadable content. For example, almost every PaC tool on the market has a canned implementation of the CIS benchmarks.

- **Break down team silos:** Use PaC to build a common workflow for automation and policy enforcement that spans I&O, security and compliance teams.

- **Integrate PaC into automation pipelines:** Use PaC to build guardrails for automation tools, so that they cannot take actions that are out of compliance.

- **Measure before and after:** Use observability tools and value stream mapping to define your starting state, then compare it to the end state. Collect real data to quantify the value of PaC.

Sample Vendors

HashiCorp; Palo Alto Networks; Progress; Pulumi; Styra

Gartner Recommended Reading

Using ‘Policy as Code’ to Secure Application Deployments and Enforce Compliance

How to Protect Your Clouds With CSPM, CWPP, CNAPP and CASB

Innovation Insight for Continuous Compliance Automation

Innovation Insight for Cloud-Native Application Protection Platforms

Magic Quadrant for DevOps Platforms

Autonomous Endpoint Management

Analysis By: Dan Wilson, Tom Cipolla

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Autonomous endpoint management (AEM) represents the AI/ML-powered convergence of DEX and UEM tool capabilities. By automating endpoint and DEX management, AEM replaces traditional tools and architectures with lightweight, cloud-based, intelligence-powered capabilities. AEM supports agile approaches, reduces IT overhead and enables efforts to be redirected toward employee enablement and business-value-added work.

Why This Is Important

Increased dependence on technology and accelerated rate of change continue to overwhelm IT, undermine technology stability and degrade DEX. AEM uses cloud-powered intelligence to automate common endpoint and experience management tasks to free up IT for more value-added work. The overall goal is to improve device stability and compliance, and employee productivity and satisfaction to drive talent attraction and retention. IT will also be viewed as a business enabler rather than a hurdle or barrier.

Business Impact

I&O leaders can automate endpoint and DEX management tasks and reallocate efforts toward business value-added work. Specific impacts include:

- Reduced IT overhead through automatic resolution of issues that disrupt and impede employee productivity.
- Maintaining endpoint configuration standards based on vendor, industry or self-defined baselines.
- Reduced cyber risk by automating patch and configuration management.
- Automated software and configuration deployment based on policy, persona or similar.

Drivers

- IT staff are overwhelmed with the growing number of endpoint devices, operating systems and applications.
- Technology vendors have accelerated development and release cadence, and IT cannot keep pace.
- Increased cyberattacks demand faster patch deployment, better device configuration compliance and closer alignment with vendor life cycles to reduce vulnerabilities.
- Adoption of UEM tools and modern management has reached critical mass as clients favor location-agnostic, cloud-based tools.
- Adoption of DEX practices and tools is growing rapidly.
- Cloud-based UEM and DEX tools are starting to demonstrate how ML-powered intelligence can quickly process a significant amount of data, provide actionable insights and recommendations, and execute automations.
- Expanding automation to perform other common administrative tasks or to apply standard policies and configurations is the next step in building toward AEM.
- Convergence could include other management tools and agents installed on endpoints.
- AEM directly supports the IT leader's goal of speed and agility.
- AEM use cases are promising in addressing the management of applications and replacing human execution of IT processes.

Obstacles

- Overly complex environments with too many disparate tools that lack integration.
- Highly customized environments that require extensive testing of every update prior to deployment.
- Fragile environments with a significant amount of technical debt — including legacy operating systems or applications that depend on unsupported browsers, runtime environments or plug-ins.
- Low- to mid-maturity organizations lack the competencies, tools and roles to ensure that more basic processes and concepts are already deployed.
- Device operating system limitations or controls may prohibit experience and automation capabilities.
- AEM tools are unlikely to address niche use cases due to insufficient data to train ML and AI models to perform the automated activities.
- AEM is not possible on-premises, so cloud-averse organizations will not be supported.
- Organizations that lack experience with agile methodologies and automation skills, and operate under a legacy mindset that focuses on control and customization.

User Recommendations

A few endpoint management vendors now offer AEM capabilities, so hype has moved slightly beyond the Innovation Trigger. Time to Plateau remains 5-10 years based on the historical adoption ramp for UEM and DEX tools. When reviewing long-term strategic plans, IT leaders should:

- Avoid lock-in by ensuring that strategic endpoint and DEX management vendors have a roadmap that directly provides or includes necessary partnerships to provide AEM capabilities.
- Reduce location dependence by migrating endpoint management, security, and identity solutions to the cloud.
- Prepare your organization by annually assessing current and future skill requirements, updating existing and defining new roles, and implementing strategies for upskilling and professional development.

- Eliminate inertia by evangelizing human-centricity and an enablement mindset, and embracing modern management principles and agile approaches.

Sample Vendors

Ivanti; VMware

Gartner Recommended Reading

Market Guide for DEX Tools

Magic Quadrant for Unified Endpoint Management Tools

Error Budgets

Analysis By: Hassan Ennaciri, Chris Saunderson

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

An error budget is a key site reliability engineering (SRE) principle used to govern how to make changes to a system, while balancing the need for rapid innovation with risk. An error budget is the number of errors a service can accumulate during a certain period without affecting users. The error budget represents the difference between "perfect" and the service-level objective (SLO).

Why This Is Important

Customers have high expectations when using digital products. They continuously demand more features in products, while expecting them to be available and reliable. Because error budgets represent the number of errors a product or service can accumulate before users start to become unhappy, they can be used to automate governance, when delivering and operating products.

Business Impact

Leveraging error budgets is an essential practice to optimize operations, maximize delivery speed and automate the governance of software releases, especially for organizations implementing DevOps and SRE practices. The primary benefit is to provide product teams with a metric that can help them balance the need to release features and introduce operational improvements, while safeguarding the SLOs.

Drivers

- **Reliability:** The main reason SRE teams use error budgets is to ensure optimal operations of systems. The acceptable levels of error offer product and operations teams flexibility to design and operate systems that are reliable and resilient within an measurable range of risks.

- **Minimized change failure rates:** Error budgets help measure high frequency of changes. while ensuring that change failure rates are maintained at or below acceptable levels.

- **Continuous improvements:** The primary goal of leveraging error budgets is to have all stakeholders embrace a culture of continuous improvements, by agreeing on target levels of acceptable errors, and collaborate to improve when the targets have been exceeded.

- **Customer expectations:** Although customers have high expectations when using digital products, they also have a certain tolerance for errors and latency. The negative impact and loyalty to products can be avoided by staying within those tolerance levels.

- **Cost optimization:** By designing and operating systems in a way that is good enough to meet customer expectations, SRE teams can optimize architectural and operational costs.

Obstacles

- **Acceptance of error budgets:** Many leaders from business and IT don't connect the term "error" with improvement or value and don't fully understand the benefits. Because of this disconnect, they resist the adoption of error budgets.

- **Skills required:** Implementing error budgets requires a mature SRE practice that many organizations lack. Experienced SRE teams are hard to find and can be expensive resources.

- **Complexity of setting and managing error budgets:** It is difficult to set error budgets initially, because they directly correlate with SLOs that are also hard to set. Targets that are too strict can affect agility and innovations, and teams would focus more on nonfunctional requirements.

- **Lack of telemetry:** Setting error rates is an onerous task to perform without sufficient historical data. This is especially challenging in complex systems with interdependencies.

User Recommendations

- **Start with teams adopting SRE practices:** Implement error budgets with product teams that have already embraced SRE practices. Start small with a few services, continuously iterate and improve to demonstrate value.

- **Educate all stakeholders:** A key to success is to educate everyone on the concept of error budgets and how this relates to customer experience (CX) and how they can be important to improving reliability. Contrast error budgets with customers' perception of value to drive home the point that error budgets need not have negative connotations.

- **Manage error budgets along with SLOs:** Like SLOs, error budgets need to be continuously evaluated and adjusted. You can't set them once and for all — they need to be reviewed periodically. It is also critical to ensure that they are consistent with customer feedback.

- **Tools and telemetry:** Invest in tools that enable SLO and error budget management, as well as tools that ingest telemetry and provide insight into error rates.

Sample Vendors

Blameless; Harness; Nobl9; SquadCast

Gartner Recommended Reading

7 Steps to Start and Evolve an SRE Practice

Improve Software Quality by Building Digital Immunity

Improve Product Reliability by Applying SRE Principles to Service Operations

Assessing Site Reliability Engineering (SRE) Principles for Building a Reliability-Focused Culture

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

Value Stream Management Platforms

Analysis By: Hassan Ennaciri, Akis Sklavounakis

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

A value stream management platform (VSMP) is a platform that seeks to optimize end-to-end product delivery and improve business outcomes. VSMPs are typically tool-agnostic. They connect to existing tools and ingest data from all phases of software product delivery — from customers' needs to value delivery. VSMPs help software engineering leaders identify and quantify opportunities to improve software product performance by optimizing cost, operating models, technology and processes.

Why This Is Important

As organizations scale their agile and DevOps practices, higher-level metrics that assess performance and efficiency of their product delivery are essential. VSMPs integrate with multiple data sources to provide DevOps-related telemetry. These insights enable stakeholders to make data-driven decisions in an agile manner and correct course as needed. The visualization capabilities of VSMPs help product teams analyze customer value metrics against the cost required to deliver that value.

Business Impact

VSMPs help organizations bridge the gap between business and IT by enabling stakeholders to align their priorities to focus on delivering customer value. VSMPs can provide CxOs with strategic views of product delivery health and pipelines, allowing them to make data-driven decisions about future product investments. These platforms also provide product teams with end-to-end visibility and insight into the flow of work to help them address constraints and improve delivery.

Drivers

- Improved software delivery with business priorities and objectives.
- Timely decision making driven by insights from data.
- Optimization of delivery flow through reduction of waste and elimination of bottlenecks.
- Visibility and mapping of end-to-end software delivery processes and identification of cross-team dependencies.
- Quality and velocity improvements of product deployments.
- More stringent governance, security and compliance requirements.

Obstacles

- VSMPs are not focused on continuous integration/continuous delivery (CI/CD) capabilities. Execution of the delivery pipeline requires use of a custom toolchain or DevOps platform.
- VSMPs require customization and data from tools used by multiple stakeholders in the organization, sometimes outside of software delivery. Collaboration with these key stakeholders to deliver the desired insights is paramount.
- VSMPs are still evolving and not all vendors have all the core capabilities.

User Recommendations

- Accelerate business outcomes by leveraging real-time, data-driven metrics and value stream insights provided by VSMPs.
- Leverage VSMPs' AI-powered analytics and insights to surface constraints, detect bottlenecks and improve flow.
- Build customized dashboards and views of product delivery for multiple stakeholders and leadership.
- Utilize VSMPs to assess the performance, quality and value of products, including development costs and ROI.
- Use VSMPs to gain a consolidated view of governance, security and compliance across all product lines.

Sample Vendors

Broadcom; ConnectALL; Digital.ai; HCLSoftware; IBM; OpenText; Opsera; Planview; Plutora; ServiceNow

Gartner Recommended Reading

Market Guide for Value Stream Management Platforms

Tools for Delivering Business Metrics to Software Engineering Teams

Market Guide for Value Stream Delivery Platforms

Use the Right Metrics in the Right Way for Enterprise Agile Delivery

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

Digital Platform Conductor Tools

Analysis By: Roger Williams, Dennis Smith

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Digital platform conductor (DPC) tools coordinate the various infrastructure tools used to plan, implement, operate and monitor underpinning technology and services for applications and digital products. They enable digital business, regardless of the environments used or who owns them. DPC tools provide a unified view of underpinning technologies and their connection to applications. This augments strategic decision making and improves the value obtained from technology investments.

Why This Is Important

Traditional, cloud and hybrid infrastructure management tools do not inherently provide an integrated view of infrastructure across all environments. Moreover, as infrastructure and operations (I&O) leaders struggle to manage their portfolio of investments to enable composable business, optimize costs and reduce risks, they need help with filling the gaps in visibility, assurance and coordination. DPC tools promise to help close these capability gaps and are improving in their ability to do so.

Business Impact

DPC tools deliver the following benefits not inherent in more focused infrastructure management toolsets:

- Visualizing digital platform performance across all life cycle stages — planning, implementing, operating and monitoring.
- Enabling continual optimal performance and placement of workloads in all environments — on-premises, in the cloud or at the edge.
- Ensuring tangible business value from improvement efforts across all technology architectures — compute, storage, middleware and network layers.

Drivers

- Difficulty in maintaining a coherent view of all technology infrastructure resources and their dependencies that are aligned with changes to services, applications and components, as well as the configuration of their promised performance levels.
- Lack of transparency into spending on hybrid digital infrastructure and how resource capacity aligns with actual application workload demand.
- Need to guide where workloads are processed (data center, public cloud, colocation facility, etc.) based on requirements, including capacity, cost and dependency dynamics.
- Challenges with estimating the value, efficiency, quality and compliance delivered by hybrid digital infrastructure based on aggregated data from performance analysis tools and other hybrid digital infrastructure management (HDIM) toolset data feeds.
- Desire for a single point of entry and reporting for digital platform resource requests, and routing them to appropriate HDIM tooling for fulfillment.
- Desire to reduce the level of skills and effort required within initiatives to improve operations and digital employee experiences.
- Gaps, duplication and conflicts in data to support application workload migration and business continuity goals, as well as protection of data from accidental deletion or malicious activities.
- Inability to confirm compliance of application workloads and digital platforms to identity requirements and security baselines as part of the organization's cybersecurity mesh approach.
- Poor credibility of business cases for digital platform improvements, including: assessing business impact; measuring gaps between current and desired performance; providing oversight of improvement efforts; and validating benefits delivered.

Obstacles

- Lack of interoperability: Tool sprawl and difficulties in integration inhibit DPC tool adoption. The technology landscape is littered with failed approaches that were intended to support data sharing between vendors.
- Lack of data credibility: The desire for a complete, accurate view of all technology as a precondition for decision making has been around for decades, yet is no closer to being realized. Customers that demand perfect data before they act, and vendors that require complete and accurate data for their tools to function properly, will continue to co-create expectations that will not be met.
- Lack of budget: DPC tools may be viewed as “overhead” that does not have a compelling business case. No one likes paying for something that does not appear to address specific pain points felt today.
- Lack of vendor commitment: Many vendors will be tempted to “DPC wash” their existing offerings and claim that these capabilities are already addressed or can be added for very little cost.

User Recommendations

- Build a DPC tooling strategy that supports digital business ambitions by defining the management elements, environments and technology layers required to meet the organization’s infrastructure needs now and in the future.
- Address measurement and coordination gaps by working with key stakeholders to identify infrastructure value and risk and cost objectives, and by making targeted investments in integration, dependency mapping and continuous improvement capabilities.
- Plan for DPC tooling investments by determining which DPC capability aspects are needed in the short, medium and long term. Compare these capabilities to current and future vendor offerings for infrastructure management tooling that can provide initial DPC tool functionality.
- Ensure that DPC tooling investments can deliver sustained value by requiring that DPC tool marketers show how the tool will address current organizational pain points and how it will adapt to future needs as organizational requirements evolve.

Sample Vendors

Cloudsoft; Flexera; HCLTech; IBM (Turbonomic); Oomnitza; OpsRamp; ReadyWorks; Snow Software; Virtana

Gartner Recommended Reading

Market Guide for Digital Platform Conductor Tools

3 Steps to Improve the Reliability of Large, Complex and Distributed IT Systems by Leveraging SRE Principles

At the Peak

Chaos Engineering

Analysis By: Jim Scheibmeir, Hassan Ennaciri

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Chaos engineering is the use of experimental and potentially destructive failure testing or fault injection to uncover vulnerabilities and weaknesses within a distributed system. Chaos engineering tools provide the ability to systematically plan, document, execute and analyze an attack on components and whole systems throughout the life cycle of the system. This planning may include the injection of random timing or attack executions.

Why This Is Important

Many organizations rely on test plans that overemphasize functionality and underemphasize validating the system's reliability and resilience. The distribution and complexity of systems makes understanding them more difficult. Chaos engineering (CE) shifts the focus of testing a system from the "happy path" toward testing how it can degrade gracefully or continue to be useful and secure while under various levels of impact. Applying CE enables improvements to system knowledge and documentation.

Business Impact

CE is aimed to minimize time to recovery and the change failure rate, while maximizing uptime and availability. Addressing these elements helps improve customer experience, satisfaction, retention and acquisition. Gartner inquiries regarding CE increased by over 11% between 2021 and 2022.

Drivers

- Increased complexity of systems and increasing customer expectations are the two largest drivers of CE and the associated tools.
- As systems become more rich in features, they also become more complex in their composition and more critical to digital business success.

- Overall, CE helps organizations become more resilient across their processes, knowledge and technology.
- Teams often lack the confidence to handle failures and the psychological safety to take action to resolve incidents. CE can help build that confidence.

Obstacles

- Within many organizations, the predominant view of CE is that the practice is random, first implemented during production, and increases, rather than reducing, risk.
- Organizational culture and attitudes toward quality and testing can present barriers to the adoption of CE. When quality and testing are only viewed as overheads, there will be a focus on feature development over application reliability.
- It can be challenging just to secure the time and budget to invest in learning CE and associated technologies. Organizations must reach minimum levels of expertise so that value is returned.

User Recommendations

- Utilize a test-environment-first approach by practicing CE in preproduction environments.
- Incorporate CE into your system development, CI/CD or testing processes.
- Build out incident response protocols and procedures, as well as monitoring, alerting and observability capabilities, in tandem with the advancement of the CE practice.
- Utilize scenario-based tests — known as “game days” — to evaluate and learn about how individual IT systems would respond to certain types of outages or events.
- Investigate opportunities to use CE in production to facilitate learning and improvement at scale as the practice matures. However, Gartner believes that very few organizations purposely use CE in their production environments.
- Formalize the practice by adopting a platform or tool to track the activities and create metrics to build feedback for continuous improvements.

Sample Vendors

Amazon Web Services; ChaosIQ; Gremlin; Harness; Microsoft; Steadybit; Verica

Gartner Recommended Reading

Quick Answer: What Metrics Should We Use to Assess and Improve Software Quality?

Predicts 2023: Observing and Optimizing the Adaptive Organization

Top Strategic Technology Trends for 2023: Digital Immune System

Predicts 2023: How Innovation Will Transform the Software Engineering Life Cycle

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

Continuous Compliance Automation

Analysis By: Daniel Betts, Hassan Ennaciri

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Continuous compliance automation (CCA) integrates compliance and security policy enforcement into DevOps delivery pipelines. CCA codifies and continuously applies compliance policies and controls, while monitoring, reporting on correcting and protecting against vulnerabilities resulting from coding defects and misconfiguration. It reduces the number of manual execution steps involved in adhering to regulatory requirements, enhancing consistency, traceability and auditability.

Why This Is Important

Increased focus on security and compliance improvements drives enterprise investments in compliance automation used to secure code and infrastructure. Traditional compliance practices are incompatible with continuous software delivery processes — leading to slower delivery and unexpected, expensive remediation work. CCA improves release velocity and reliability while simplifying compliance enforcement and reporting via policy-driven, automated controls.

Business Impact

Organizations' evolving DevOps/DevSecOps practices can minimize risks and penalties by embedding automated compliance and reporting into their delivery pipelines. CCA enables organizations to integrate compliance into all phases of the delivery pipeline and consistently enforces compliance policies without sacrificing operational agility. CCA tools can offer benchmarks, assessments and self-service reporting to enable efficiencies in compliance auditing.

Drivers

- As organizations face an increasing number of regulatory obligations and more stringent enforcement, automating compliance will become even more valuable to I&O leaders as they strive to maximize flow.
- Additional compliance requirements continue to be added and require support with limited delay.
- Compliance activities are increasingly executed through automated testing, which delivers increased efficiency for developers and reduces the risk of compliance audit failures.
- As cloud-native application architectures and development models become more pervasive, integrating compliance into the toolchain will become more feasible and common.
- Compliance reporting, benchmarking and assessments are often manual and slow.

Obstacles

- No vendor provides capabilities across all elements of the delivery value stream. DevOps teams must integrate multiple tools into their value streams to provide compliance coverage across development and delivery activities.
- Failure to engage with compliance and security subject matter experts (SMEs) early in the development life cycle can lead to problems.
- A lack of rule set understanding and consistent implementation can be an impediment to CCA. Failure to consistently involve organizational compliance teams in implementation leads to a failure in delivering maximum value.
- Poorly implemented CCA presents a business risk. If it is assumed that by implementing CCA, delivered software becomes compliant without additional effort, organizations will face increased risk of compliance failure.

User Recommendations

- Adhere to compliance, governance and security requirements while creating a leaner operating environment.
- Implement a shift-left approach to ensure compliance controls are understood and applied earlier in the development process. Implement automated compliance checks at every phase of the pipeline, demonstrating a “shift secure” approach.
- Invest in tools that enable CCA at scale and can provide a continuous approach to prevent, detect and correct audit failures, and remove manual reporting activities.
- Select tools that can integrate into DevOps delivery platforms to enable security and compliance checking.
- Enforce security and compliance across all domains, including databases, application code, infrastructure and open-source software. No single vendor tool covers all these domains, so DevOps teams must use multiple tools and integrate across all phases of the delivery pipeline.
- Enable efficient compliance policy checking through compliance automation tools to measure benchmarks, perform assessments and report on compliance policy controls.

Sample Vendors

Anitian; Contrast Security; JFrog; Mend.io; Rapid7; Redgate; RegScale; Snyk; Sonatype; Styra

Gartner Recommended Reading

Market Guide for Continuous Compliance Automation Tools in DevOps

3 Essential Steps to Enable Security in DevOps

How to Build and Evolve Your DevOps Toolchains

Market Guide for Value Stream Delivery Platforms

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

DevOps Platforms

Analysis By: Manjunath Bhat

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

DevOps platforms provide fully integrated capabilities to enable continuous delivery of software using agile and DevOps practices. These span the software development life cycle (SDLC) and include product planning, version control, continuous integration, test automation, continuous deployment, release orchestration, automating security and compliance policies, monitoring, and observability. DevOps platforms support team collaboration, secure software development and software delivery metrics.

Why This Is Important

Organizations use DevOps platforms to minimize tool friction and operational complexity resulting from disparate toolchains, manual handoffs, and lack of consistent visibility throughout the SDLC. This enables product teams to deliver faster customer value without compromising quality. The DevOps platforms market reflects the consolidation of technologies across development, security, infrastructure and operations to streamline software delivery.

Business Impact

DevOps platforms are the software delivery pipelines that enable continuous delivery of business value. The seamless integration, automation, extensibility and shared visibility between development, security and operations workflows help bridge the silos that exist between these teams. Using a common platform for development, security and operations accelerates agile transformation, and helps organizations move toward a product and platform team operating model.

Drivers

- **Modernizing application architectures:** Modernizing applications to take advantage of emerging cloud-native architectures requires fundamental changes to underlying DevOps practices and tools.

- **Increased emphasis/focus on enhancing developer experience:** Improved developer experience, agility and the need to improve delivery cadence by reducing cognitive load due to constant context switches and repetitive low-value work.

- **An integrated approach to security and compliance:** Integrating and automating security, compliance and governance as part of the development and delivery process is becoming a priority. A few DevOps platform providers include SCA capabilities as features in their offerings. Example vendors include GitHub, GitLab and JFrog.

- **Improved visibility into the flow of work:** Organizations are under pressure to reduce friction and manual handoffs, and this requires complete visibility into software delivery pipelines from ideation to production.

Obstacles

- Organizations that want to unlock the full benefits of DevOps platforms must be willing to replace an existing toolchain — either completely or in part. Teams can view the change as a disruption to their established ways of working and resist any change to the tools they have been using.

- Organizations accrue technical and skill debt over time due to outmoded automation workflows and legacy applications. This hinders teams from adopting new tools.

- Dependency on a single provider for a majority of their software development needs increases concentration risk and lowers bargaining leverage.

- Most DevOps platforms currently fall short in providing the full set of software delivery capabilities that organizations require to build, deliver, measure and improve the flow of value in the software delivery life cycle.

User Recommendations

- To fully reap the business benefits of DevOps platforms, organizations must adopt agile methods and practices.
- Scale and deliver capability by providing DevOps platforms as self-service platforms to reduce overhead, lower complexity, and ensure consistent and templatized workflows across multiple teams.
- Improve the flow of value by streamlining the software delivery life cycle with DevOps platforms that provide enhanced visibility, traceability, auditability and observability across the DevOps pipeline.
- Support InnerSource efforts by building InnerSource portals using source control repositories available in DevOps platforms.
- Reduce inconsistency in CI/CD pipeline definitions between teams by leveraging declarative and shareable pipeline capabilities in DevOps platforms.

Sample Vendors

Atlassian; CircleCI; CloudBees; GitHub; GitLab; Harness; JetBrains; JFrog; Red Hat; VMware

Gartner Recommended Reading

Keys to DevOps Success

Research Roundup for DevOps, 2022

DEX Tools

Analysis By: Dan Wilson, Autumn Stanish, Stuart Downes, Tom Cipolla

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Digital employee experience (DEX) tools help IT leaders measure and continuously improve the performance and employee sentiment toward company-provided technology. Near-real-time processing of aggregated data from endpoints, applications, employee sentiment and organizational context surfaces actionable insights and drives self-healing automation, optimized support and employee engagement. Insights and self-healing can also enhance IT support.

Why This Is Important

Accelerated digital workplace investment has highlighted gaps in objective measurement and continuous improvement of DEX. Client interest in DEX has steadily increased since the start of 2021. Primary use cases focus on tactical and technology issues however mature digital workplaces are expanding to include more strategic use cases. Their cross-functional DEX strategy directly targets reduced IT overhead and improved DEX as a way to retain and attract top talent.

Business Impact

DEX tools shift focus from technology management to more business value-added work. Specific impacts include:

- Fewer IT issues that disrupt and impede employee productivity.
- Reduced IT overhead through automation.
- Improved endpoint configuration and patch compliance.
- Better balance of objective and subjective success measures, including technology adoption, performance and employee sentiment.
- IT becoming more proactive and human-centric.
- Increased ability to retain talent.

Drivers

- DEX is a major influencer of the overall employee experience.
- Organizations are increasingly dependent on technology to perform their work.
- Employees are suffering in silence by living with or working around issues rather than reporting issues to IT.
- IT leaders seek broader measurement and management capabilities as internally focused activity KPIs have proven incomplete.
- IT administrators are looking for better visibility into how hybrid workers' devices are performing.
- Employee sentiment toward technology cannot be measured effectively with periodic or transactional surveys alone. Feedback must also include how employees feel about and engage with specific devices or apps, and how technology changes impact their work.
- Service desk and other IT support analysts require faster access to device configuration and performance data to offset an increase in support interaction volumes and wait times.
- Increasing threat of cyberattacks demands faster identification and remediation of configuration issues and missing patches.
- Increased focus on sustainable IT is promoting consumption- and performance-based device life cycles in place of refreshing devices on a schedule.
- AI and machine learning have significantly increased the value and capability of SaaS-based DEX tools.

Obstacles

- Legacy culture that does not trust the tool's insights or sees automation as a threat.
- SaaS- or cloud-averse organizations will be limited to less capable on-premises offerings.
- Low-maturity IT support or end-user computing (EUC) organizations may not be ready for DEX tools.
- An "ignorance is bliss" mindset fearing that a sudden unveiling of the massive volume issues will make IT leadership look bad.
- The cost to acquire, implement and integrate new tools.
- Insufficient staffing levels or skills required to operate a DEX tool.
- Failure to adjust IT staff rewards and recognition to promote new behaviors and DEX tool adoption.
- The need to account for legislative, regulatory, industry or labor union limits on data collection and use.
- The lack of maturity and feature parity among representative and similar tools including common APIs for integration.
- Smaller organizations have limited options given that many DEX tools target larger enterprises.

User Recommendations

In its third year on the Hype Cycle, DEX tools have reached the Peak of Inflated Expectations. Market penetration and maturity have also advanced. Organizations that have not invested in DEX tools should:

- Build a broader team by collaborating with business and IT peers to define IT and non-IT use cases.
- Ensure the business case focuses on objective and measurable impacts by minimizing reliance on vendor-provided ROI templates.
- Choose a DEX tool that best fits your needs and budget by using the Market Guide for DEX Tools.

- Assign dedicated ownership and allocate dedicated resources to deploy and drive DEX tool adoption and ROI. Resources can be reallocated from IT support roles as proactive automation reduces support volumes.
- Incentivize new behaviors by adapting IT performance measures to focus more on outcomes than activities.
- Avoid diminishing returns by adding features and use cases as the team and DEX tool matures.

Sample Vendors

1E; ControlUp Technologies; HP Inc.; Ivanti; Lakeside Software; Nanoheal; Nexthink; Riverbed Technology; Tanium; VMware

Gartner Recommended Reading

How to Successfully Deploy a DEX Tool

Market Guide for DEX Tools

Employee Enablement Is Key to Digital Workplace Services Leaders' Survival

SMP

Analysis By: Dan Wilson, Jaswant Kalay, Tom Cipolla, Sid Nag

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

SaaS management platforms (SMP) help IT discover, manage, automate, operate, optimize and govern organizationwide SaaS use from a centralized console. SMPs also enhance protection of identities and data while using SaaS and SMP's enable SaaS operations — which include the capabilities supporting IT operations, PlatformOps, SecOps and site reliability engineering (SRE). Though SMP vendors focus on operational management or optimization of SaaS, a few have emerged to address both.

Why This Is Important

As SaaS adoption accelerates and managing spend becomes difficult, IT leaders are challenged with discovering and supporting SaaS in accordance with company, market or geographic policy and regulations. The increase in cyberattacks focuses attention on protecting identity and data in SaaS. These trends continue to attract new SMP market entrants, investment and M&A. The SMP market remains fragmented and difficult to navigate, and hyperscale cloud providers approaches differ substantially.

Business Impact

IT leaders can leverage SMP to:

- Improve Saas visibility and manageability
- Reduce or optimize costs
- Improve management of SaaS contracts and renewals, and optimize costs
- Reduce business-acquired SaaS by offering app-store experiences for employees
- Streamline new SaaS onboarding
- Reduce IT overhead with automation
- Improve employee on/offboarding workflows
- Promote collaboration between teams in the SaaS life cycle

Low Gartner client interest keeps hype parked at the peak. Plateau time has been extended, and market penetration and maturity are unchanged from 2022.

Drivers

- SaaS spend continues to grow by 15-20% annually, as organizations maintain an average of over 125 different SaaS applications totaling $1,040 per employee annually.
- IT typically is aware of only a third of those due to decentralized ownership and sourcing.
- SMPs also report that less than half of provisioned subscription-based licenses are regularly used by employees.
- IT teams responsible for discovering, managing, automating, optimizing, protecting and governing SaaS struggle to effectively do this through native SaaS administrator consoles.
- Harmonizing SaaS configurations and employee on/offboarding are also common pain points.
- SMP adoption is higher in small to midsize organizations, as centralized responsibility for SaaS is more common.
- Clients are also struggling to choose between SMP, SaaS security and SAM tools. All three offer SaaS discovery, protection and some optimization capabilities — however, SMPs can do more.
- A lack of common APIs or controls means that SMPs have varying levels of integration and capability to manage and automate SaaS applications.
- Utility continues to improve as new entrants to the SMP and adjacent markets promote unique new capabilities.
- I&O leaders don't have the available tools and capabilities for observability, application monitoring, cost, license or configuration management, and security visibility for this new world of applications. There is no integrated platform approach to these functionalities and tools.
- Broader SaaS operations capabilities to support IT operations, PlatformOps, SecOps and SRE services, as well as continuous integration/continuous delivery (CI/CD) pipelines and other agile approaches.

Obstacles

- Decentralized or shared responsibility within organizations complicates buying decisions.
- Many organizations underestimate SaaS sprawl and do not fully understand how an SMP can help.
- Low maturity organizations generally see SMP as too advanced and have more basic priorities.
- Costs associated with assessing, selecting, implementing and staffing resources to utilize SMP are rarely allocated in budgets.
- Varying breadth and depth of SaaS coverage and integrations. SaaS-heavy organizations often find that SMPs do not cover all of their applications and licensing models.
- Capability overlaps with SAM and SaaS security tools.
- Concerns about the addition of another management tool.
- The SaaS management market is highly fragmented and characterized by wide variability and only partial overlap between tools.
- Gartner client interest remains low compared to other digital workplace tool conversations.
- DevOps, apps, digital workplace and I&O teams generally operate in silos.
- Managing configurations for dozens to hundreds of SaaS apps using their separate admin consoles is untenable.
- Confusion and the business acquiring their own applications, due to a decentralized approach with no clear owner. This results in uncontrolled cost, identity and data security exposure, missing observability and service management processes.

User Recommendations

IT leaders responsible for managing SaaS should:

- Implement an overall SaaS operations strategy and execution plan.
- Avoid overspending by focusing first on discovery.

- Build a business case to fund the SMP by utilizing optimization capability to reduce unnecessary spend on unused and underutilized licenses, and to consolidate similar apps.
- Uncover unsanctioned SaaS by using an SMP with strong discovery capabilities through desktop agents, browser extensions and deep integration with security and finance tools.
- Minimize risk by finding and addressing SaaS that is not integrated with identity and SSO solutions, and documenting discovered SaaS in enterprise architecture tools or CMDBs.
- Choose an SMP that best fits your requirements by reviewing integrations with critical apps to understand if the SMP offers read and write functionality, or is limited to pulling reports.
- Bring together disparate IT teams and processes.

Sample Vendors

Beamy; BetterCloud; LeanIX; Productiv; SailPoint; Snow Software; Torii; Trelica; Zluri; Zylo

Gartner Recommended Reading

Market Guide for SaaS Management Platforms

Market Guide for Software Asset Management Tools

Infographic: Why Are You Wasting Your SaaS Expenditure?

How to Establish Effective SaaS Governance

Observability

Analysis By: Padraig Byrne, Gregg Siegfried

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Observability is the characteristic of software and systems that enables them to be understood, based on their outputs and enables questions about their behavior to be answered. Tools that facilitate software observability enable observers to collect and quickly explore high-cardinality telemetry using techniques that iteratively narrow the possible explanations for errant behavior.

Why This Is Important

The inherent complexity of modern applications and distributed systems and the rise of practices, such as DevOps, has left organizations frustrated with legacy monitoring tools and techniques. These can do no more than collect and display external signals, which results in monitoring that is, in effect, only reactive. Observability acts like the central nervous system of a digital enterprise. Observability tools enable a skilled observer to explain unexpected system behavior more effectively.

Business Impact

Observability tools have the potential to reduce both the number of service outages and their severity. Their use by organizations can improve the quality of software, because previously invisible (unknown) defects and anomalies can be identified and corrected. By enabling product owners to better understand how their products are used, observability supports the development of more accurate and usable software, and a reduction in the number and severity of events affecting service.

Drivers

- The term “observability” is now ubiquitous, with uses extending beyond the domain of IT operations. Although the 2020s are now the “decade of observability,” care must be taken to ensure the term retains relevance when used beyond its original range of reference.

- OpenTelemetry’s progress and continued acceptance as the “observability framework for cloud-native software” raises observability and its toolchain.

- Traditional monitoring systems capture and examine signals (possibly adaptive) in relative isolation, with alerts tied to threshold or rate-of-change violations that require prior awareness of possible issues and corresponding instrumentation. Given the complexity of modern applications, it is unfeasible to rely on traditional monitoring alone.

- Observability tools enable a skilled observer, a software developer or a site reliability engineer to explain unexpected system behavior more effectively, provided enough instrumentation is available. Integration of software observability with artificial intelligence for IT operations (AIOps) to automate subsequent determinations is a potential future development.

- Observability is an evolution of longstanding technologies and methods, and established monitoring vendors are starting to reflect observability ideas in their products. New companies are also creating offerings based on observability.

Obstacles

- In many large enterprises, the role of IT operations has been to “keep the lights on,” despite constant change. This, combined with the longevity of existing monitoring tools, means that adoption of new technology is often slow.

- Enterprises have invested significant resources in their existing monitoring tools, which exhibit a high degree of “stickiness.” This creates nontechnical, cultural barriers to adopting new practices such as those based on observability.

- Costs associated with observability tools have grown as companies struggle to keep up with the explosion in volume and velocity of telemetry.

User Recommendations

- Assess software observability tools to integrate into their continuous integration/continuous delivery (CI/CD) pipelines and feedback loops.
- Investigate problems that cannot be framed by traditional monitoring by using observability to add flexibility to incident investigations.
- Enable observability by selecting vendors that use open standards for collection, such as OpenTelemetry.
- Tie service-level objectives to desired business outcomes using specific metrics, and use observability tools to understand variations.
- Ensure IT operations and site reliability engineering teams are aware of updates to existing monitoring tools and how they may take advantage of them. Many traditional application performance monitoring vendors are starting to incorporate observability features into their products.
- Avoid the conclusion that observability is synonymous with monitoring. At minimum, observability represents the internal perspective, rather than external.

Sample Vendors

Chronosphere; Grafana; Honeycomb; Lightstep; Observe; VMware

Gartner Recommended Reading

Monitoring and Observability for Modern Infrastructure and Applications

Magic Quadrant for Application Performance Monitoring and Observability

Intelligent Infrastructure

Analysis By: Philip Dawson, Nathan Hill

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Emerging

Definition:

Intelligent infrastructure is built from simple, repeatable infrastructure building block components, integrated and managed in a standardized, automated manner. It optimizes infrastructure resources for application consumption through infrastructure machine learning (ML) and tuning as software overlays through an automated software intelligence plane.

Why This Is Important

Intelligent infrastructure encapsulates generative AI and ML into the infrastructure configuration. Building on the capabilities of virtualization, it adds the dynamic hardware composition capability of a composable infrastructure to deliver a hardware configuration that is optimized for a specific application. Intelligent infrastructure additionally adds or feeds the generative AI/ML automation functions to the intelligence plane.

Business Impact

Intelligent infrastructure is an innovation in delivering automated optimized systems for application delivery. It builds on earlier innovations, including converged, hyperconverged, software-defined and composable infrastructures, helping deliver hybrid cloud-like infrastructure on-premises or with a provider. It feeds off the application API-led programmable infrastructure that tunes infrastructure through system calls and requests, which improves application and infrastructure integration.

Drivers

- IT leaders now recognize that cloud infrastructure, cloud platforms and cloud-native applications drive the overall composable, programmable and intelligent infrastructure journey.

- Cloud delivery and edge expansion are fueling the standardization of infrastructure, design and architecture and the expansion of the three areas to edge and Internet of Things (IoT) locations beyond remote offices/branch offices (ROBOs).

- Adding generative AI and automation on top of this infrastructure composition capability ensures that infrastructure is always optimized for the application load.

- In intelligent infrastructure, the “control plane” is enhanced with automation driven by infrastructure analytics ML, to become an automated “intelligence plane.”

Obstacles

- The intelligence plane automates infrastructure and workload provisioning to application consumption. Intelligent infrastructure should not be tied to hardware features, but rather software functions.
- As with software-defined and composable infrastructures, traditional system vendors often tie intelligent infrastructure to hardware-related features, which can propel lock-in.
- Cloud management platforms are used as overlays for cloud migrations. Intelligent infrastructure has to adapt to hybrid cloud and multicloud delivery, delivering client value whether on-premises, with a provider or public cloud through anything as a service (XaaS).

User Recommendations

- Select infrastructure solutions based on their ability to meet the current business requirements while still offering the flexibility to exploit the integration and automation of intelligent infrastructure innovations to be delivered over the next five years.
- Increase agility and business alignment by integrating application, asset management and sourcing information into the infrastructure intelligence and control planes as a drive to platform- and infrastructure-driven consumption models.
- Prepare for the evolution of application delivery and workload provisioning by incorporating intelligence/ML infrastructure functions with intelligent fabrics into your future system requirements.

Sample Vendors

Cisco; CU Coding; Hewlett Packard Enterprise; IBM; Intel; Microsoft; Tintri; VMware

Gartner Recommended Reading

How to Evolve Your Physical Data Center to a Modern Operating Model

Market Guide for Servers

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

Sliding into the Trough

Cloud Data Backup

Analysis By: Jerry Rozeman

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Cloud data backup tools back up and restore production data generated in the cloud. Data can be created by SaaS tools (e.g., Microsoft 365); platform as a service (PaaS) tools (e.g., Amazon Relational Database Service [RDS]); or infrastructure as a service (IaaS) tools (e.g., Amazon Elastic Compute Cloud [EC2]). Backup copies can be stored in the same or a different cloud location, or on-premises in the data center, where restore granularity/recovery location options should be offered.

Why This Is Important

Public cloud providers typically offer infrastructure resilience and availability to protect their systems from server, site or region failures, and generally provide shared responsibility for the data. When data is lost due to user or administrator error, configuration and patching changes, development issues, software corruption, or malicious attacks, user organizations are responsible, rather than the cloud provider. Cloud data backup tools address these deficiencies.

Business Impact

Adopting cloud data backup tools will deliver:

- Confidence in routine data backup of critical computing and application data
- The ability to comply with data protection policies
- Improved availability of data to recover after infrastructure failure, user or administrator errors, software corruption, or malicious attacks

Drivers

- As more production workloads migrate to the cloud (in the form of SaaS, PaaS or IaaS), it has become critical to protect the data generated natively in the cloud.
- Cloud providers focus on infrastructure high availability and disaster recovery (DR), but are not responsible for application or user data loss.
- Most SaaS applications' natively included data protection capabilities are not true backup, and lack secure access control and consistent recovery points to recover from internal and external threats.
- As Microsoft 365 is widely adopted, the need for better protection is growing rapidly, which is especially driven by Microsoft's inconsistent and incomplete use of recycle bins, the requirement for retention policies, and lack of intuitive recovery processes.
- Backup of Salesforce data is the second-most-addressed workload by vendors in this space.
- Native backup of IaaS and PaaS data usually resorts to cloud-based snapshots and scripting, which may lack application consistency, restore options, data mobility, storage efficiency and policy-based automation, and do not provide a secure, independent external copy of the data.
- Interest in providing backup for Azure AD, Azure DevOps and GitHub is rising.

Obstacles

- Deploying data protection for cloud-based workloads is often an afterthought, because it is not part of the original business case for cloud-based workload deployment or migration.
- In-depth review of each cloud vendor's SLAs is another obstacle that customers have to overcome, because it limits them in their speed of cloud adoption.
- The outcome of the SLA review might block the cloud service adoption because the SLA might not meet company requirements.
- Besides Microsoft 365 and Salesforce, most SaaS-based applications do not support third-party, external backup solutions that limit customers in protecting these workloads.
- Adopting cloud data backup tools will require significant investments in software, services and/or infrastructure, knowledge and processes.

- Establishing partnerships by IT with apps, DevOps and other teams to structure data protection can be a challenge.

User Recommendations

- Ensure that an enterprise-class data backup and recovery strategy is part of every cloud deployment or migration, which aligns with organizational compliance requirements.
- Evaluate and thoroughly understand cloud-native backup and recovery capabilities, and compare them with your company protection policies before migrating applications to SaaS, PaaS or IaaS data infrastructure solutions.
- Ensure that contracts with cloud providers clearly specify the capabilities and costs associated with the backup solution, including exit fees, and understand the limitations of such solutions.
- Factor in the cost of cloud backup application, in addition to the cost of hosting the production application in the cloud.
- Focus on ease of deployment, ease of management, data mobility, storage efficiency and flexible options in terms of backup/recovery granularity and location when selecting third-party backup tools.

Sample Vendors

AvePoint; Cohesity; Commvault; Druva; HYCU; Keepit; OwnBackup; Rubrik; Veeam; Veritas

Gartner Recommended Reading

Magic Quadrant for Enterprise Backup and Recovery Software Solutions

Critical Capabilities for Enterprise Backup and Recovery Software Solutions

Market Guide for Backup as a Service

Innovation Insight: Backup for SaaS Applications

Quick Answer: Should I Back Up Microsoft 365?

Site Reliability Engineering

Analysis By: George Spafford, Daniel Betts

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Site reliability engineering (SRE) is a collection of systems and software engineering principles used to design and operate scalable resilient systems. Site reliability engineers work with the customer or product owner to understand operational requirements and define service-level objectives (SLOs). Site reliability engineers work with product or platform teams to design and continuously improve systems that meet defined SLOs.

Why This Is Important

SRE emphasizes the engineering disciplines that lead to resilience; but individual organizations implement SRE in widely varying ways such as a defined role or a set of practices. SRE teams can serve as an operations function, and nearly all such teams have a strong emphasis on blameless root cause analysis. This is to decrease the probability and/or impact of future events and to enable organizational learning, continual improvement and reductions in unplanned work.

Business Impact

The SRE approach to improving reliability and resilience is intended for products and platforms that need to deliver customer value at speed at scale while managing risk. The two primary use cases are to improve the reliability of existing products/platforms or to create new products or platforms that need reliability from the start.

Drivers

- Clients are under pressure to meet customer requirements for reliability while scaling their digital services and are looking for guidance to help them.

- While Google originated what became known as SRE and continued to evolve it, practitioners are developing and sharing new practices as well. Potential practitioners looking for pragmatic guidance to improve the reliability of their systems have a rich body of knowledge they can leverage that works well with agile and DevOps.

- Organizations are adopting highly skilled automation practices (usually DevOps), and usage of infrastructure-as-code capabilities (which usually requires a cloud platform) to deliver digital business products reliably.

- The most common use case based on inquiry calls with clients is to leverage SRE concepts to improve the reliability of existing systems that are not meeting customer requirements for availability, performance or are proving difficult to scale.

Obstacles

- Insufficient internal marketing to understand what agile, DevOps or product teams need or would value and then explaining how the value SRE can deliver will justify the costs and risks incurred. Without marketing its benefits, SRE adoption tends to be less certain or slower. The SRE concept by itself is insufficient — people must continuously believe it is worthwhile.

- Finding SRE candidates who have the right mix of development, operations and people skills is a big challenge for clients. Impacts on initial adoption and scaling efforts as well.

- Rebranding of a traditional operations team without changing to adopt SRE practices, only SRE in name.

- Clients have voiced problems with product owners who overly focus on functional requirements and not nonfunctional requirements thus slowing improvements and support of SRE within the organization.

User Recommendations

- Leverage practices pragmatically based on need. Don't feel that you must implement SRE exactly the way Google does it, learn what works for you.
- Detect an opportunity to begin that is politically friendly, will demonstrate sufficient value and has an acceptable risk profile.
- Start small, focus, learn, improve, and demonstrate value — do not try to change everything at once.
- Work with the customer or product owner to define clear, obtainable SLOs based on their needs.
- Implement monitoring and improve observability to objectively report on actual performance relative to the SLOs.
- Product owners must be accountable for functional and non-functional requirements of their products.
- Instill collaborative working between site reliability engineers, developers and other stakeholders to help them learn how to design, build and evolve their products to meet SLOs.
- Create a community, implement effective organizational learning practices and evolve SRE practices.

Sample Vendors

Atlassian; Blameless; Datadog; Dynatrace; New Relic; OpsRamp; PagerDuty; Splunk

Intelligent Automation (I&O)

Analysis By: Chris Saunderson

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Intelligent automation (IA) for infrastructure and operations (I&O) is the application of AI techniques, advanced rule engines, heuristics and machine learning (ML) to automate decision making and execute actions for I&O activities. It involves collection, analysis, recommendations, and actions based on data gathered from human and machine-based sources. IA is increasingly being used to improve business agility and reduce outage impact, and is driving more advanced I&O service enablement.

Why This Is Important

I&O leaders are increasingly looking to ML-based analytics and augmented decision making to improve operational resiliency and responsiveness, address complexity and process increasingly large amounts of data through automation. In keeping with the demand in the market, technology providers are adjusting their product focus to apply analytics techniques, such as decision trees, knowledge graphs, clustering, regression and classification.

Business Impact

I&O teams should be in lockstep with their business to ensure performance, reliability and resilience needs are met. IA drives data collection, updates, analysis and automation of actions. This enables new automated capabilities that deliver:

- Predictive capabilities: maintenance/failure effects, cost/delivery forecasting.
- Staff efficiency: value-added work rather than manual work, root cause analysis.
- Insight generation: trends, recommendations for next automation actions, unhandled event analysis.

Drivers

- IA is an approach that is being investigated by clients to optimize their service operation costs by eliminating manual tasks, and to enable scalable operational support at a manageable cost.
- Technology providers that offer best-of-breed tools for artificial intelligence for IT operations (AIOps), application performance monitoring (APM) and robotic process automation (RPA) will influence IA. AIOps and stand-alone RPA technology providers may expand their offerings to deliver IA, through acquisitions or organic development. Typically, infrastructure managed service providers (MSPs) source third-party IA solutions to expand capabilities in their service offerings.
- Maturation of the use of automation will increase reliability and velocity of delivery, and cost optimization, and reduce toil for operations teams and cognitive loads on platforms and operations teams.
- Three factors drive synergy among IA, AIOps and RPA: the buying segment (I&O leaders) overlaps across these technologies; the objectives (increasing efficiency, scale and agility) are aligned; and the future of these innovations will increasingly be driven by AI technologies.

Obstacles

- Successful implementation of IA will leverage a high degree of cooperation and trust between business, I&O, data and analytics teams, and technology providers.
- IA for I&O has significant overlaps with multiple automation domains that present challenges in identifying suppliers that can fill distinct I&O use cases without duplication. IA tool providers offer the underlying algorithmic implementations, connectors and data repositories, but the implementation still requires significant setup and refinement, and is never “out of the box.”
- There is pressure to use existing automation solutions to address IA use cases, even if only partially successful. The costs of these solutions, especially related to the skills investment needed, are challenging to justify.
- Required cross-domain skills for developing solutions to meet the challenges of the complex environment into which these platforms are targeted may place the I&O organization at a disadvantage in securing the talent and skills needed.

User Recommendations

- Define use cases by analyzing gaps in existing automation that can benefit from augmented decision making and execution.
- Collaborate with data and analytics teams to adapt best practices that include data preparation, cleansing and data lakes to glean insights from a centralized knowledge repository. Development of skills to identify root cause for AI-derived exceptions will be key.
- Leverage I&O procedures and documentation to help train and sustain AI models. Leverage investments in infrastructure MSPs that offer IA solutions or partner with stand-alone IA tool providers.
- Roadmap the adoption of IA as an evolution of your automation journey, keeping humans in the loop until confidence is built, and transition your team to an automation engineering role,

Sample Vendors

arago; AutomationEdge; Coretex; CSS Corp; HCL Technologies; NTT DATA; Perpetuuiti; Tata Consultancy Services

Programmable Infrastructure

Analysis By: Philip Dawson, Nathan Hill

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Programmable infrastructure is the concept of using and applying methods and tooling from the software development area to management of IT infrastructure. This includes, but is not limited to, APIs, immutability, resilient architectures and agile techniques.

Why This Is Important

Programmable infrastructure ensures optimal resource utilization, while driving cost efficiencies. A continuous delivery approach requires continuous insight and the ability to automate application responses. Moving to an API-driven infrastructure is the key first necessary step to enabling anti-fragile and sustainable automation through programmatic techniques.

Business Impact

Greater value (rather than cost reduction) is achieved via programmable infrastructure's ability to drive adaptive automation — responding faster to new business infrastructure demands, driving service quality and freeing staff from manual operations. Programmable infrastructure reduces technical debt with investment and enables a sustainable and highly responsive IT infrastructure service to the business.

Drivers

- Programmable infrastructure strategies are applied to private cloud, hybrid cloud and infrastructure platforms as well as public cloud. Demand for programmable infrastructure grows as heterogeneous infrastructure strategies are embraced.
- Programmable infrastructure is needed to manage the life cycle of infrastructure delivery from provisioning, resizing and reallocation to reclamation, and in the case of external resources, manage elasticity and the termination of consumption.
- Programmable infrastructure is needed to optimize and reduce the dependency on the infrastructure life cycle. More importantly, it enables the desired (performance, cost, speed) infrastructure provisioning and orchestration in line with business demands.

Obstacles

- The ongoing cost of refreshing API-enabled infrastructure components on-premises after initial implementation adds financial pressure to organizations.
- Applying automation to existing monolithic infrastructure components fails due to the lack of platform agility and vendor lock-in.
- While APIs enable integration across different infrastructure platforms, the lack of open APIs/API compatibility across vendor platforms creates a siloed mentality.
- The implementation of programmable infrastructure is hampered by the early adoption of it within infrastructure and operations (I&O), and the shortage of skilled software engineering resources to comprehensively exploit it (especially in web technologies such as HTTP and JSON to develop these APIs).

User Recommendations

- Deploy a programmable infrastructure to further abstract application from infrastructure delivery and pursue an agile digital business outcome.
- Implement a programmable infrastructure by investing in infrastructure automation tools and continuous delivery (example vendors for these markets are listed below, but no single vendor or platform can enable an organizationwide programmable infrastructure strategy) leading to API-led programmable platforms.
- Invest in infrastructure and DevOps, and modernize legacy IT architectures to implement an API-driven infrastructure.
- Examine reusable programmable infrastructure building blocks leveraging programmable infrastructure strategy built on repeatable and available skills from providers.

Sample Vendors

Amazon Web Services; CU Coding; Google; IBM; Microsoft; Oracle; Quality Technology Services; RackN; Tencent; VMware

Gartner Recommended Reading

Market Guide for Servers

Predicts 2023: XaaS Is Transforming Data Center Infrastructure

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?

Container Management

Analysis By: Dennis Smith, Michael Warrilow

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Gartner defines container management as offerings that enable the development and operation of containerized workloads. Delivery methods include cloud, managed service and software for containers running on-premises, in the public cloud and/or at the edge. Associated technologies include orchestration and scheduling, service discovery and registration, image registry, routing and networking, service catalog, management user interface, and APIs.

Why This Is Important

Container management automates the provisioning, operation and life cycle management of container images at scale. Centralized governance and security are used to manage container instances and associated resources. Container management supports the requirements of modern applications, including platform engineering, cloud management and continuous integration/continuous delivery (CI/CD) pipelines. Benefits include improved agility, elasticity and access to innovation.

Business Impact

Industry surveys and client interactions show that demand for containers continues to rise. This trend is due to application developers' and DevOps teams' preference for container runtimes, which use container packaging formats. Developers have progressed from leveraging containers on their desktops to needing environments that can run and operate containers at scale, introducing the need for container management.

Drivers

- The adoption of DevOps-based application development processes.
- The rise of cloud-native application architecture based on microservices.
- New system management approaches based on immutable infrastructure, which gives the ability to update systems frequently and reliably maintained in a “last known good state” rather than repeatedly patched.
- Cloud-based services built with replaceable and horizontally scalable components.
- A vibrant open-source ecosystem and competitive vendor market have culminated in a wide range of container management offerings. Many vendors enable management capabilities across hybrid cloud or multicloud environments. Container management software can run on-premises, in public infrastructure as a service (IaaS), or simultaneously in both.
- Container-related edge computing use cases have increased in industries that need to get compute and data closer to the activity (for example, telcos, manufacturing plants, etc.).
- AI/ML use cases have emerged over the past few years, leveraging the scalability capabilities of container orchestration.
- Cluster management tooling that enables the management of container nodes and clusters across different environments is increasingly in demand.
- All major public cloud service providers now offer on-premises container solutions.
- Independent software vendors (ISVs) are increasingly packaging their software for container management systems through container marketplaces.
- Some enterprises have scaled sophisticated deployments, and many more are planning container deployments. This trend is expected to increase as enterprises continue application modernization projects.

Obstacles

- More abstracted, serverless offerings may enable enterprises to forgo container management. These services embed container management in a manner that is transparent to the user.
- Third-party container management software faces huge competition in the container offerings from the public cloud providers, both with public cloud deployments and the extension of software to on-premises environments. These offerings are also challenged by ISVs that choose to craft open-source components with their software during the distribution process.
- Organizations that perform relatively little app development or make limited use of DevOps principles are served by SaaS, ISV and/or traditional application development packaging methods.

User Recommendations

- Determine if your organization is a good candidate for container management software adoption by weighing organizational goals of increased software velocity and immutable infrastructure, and its hybrid cloud requirements, against the effort required to operate third-party container management software.
- Leverage container management capabilities integrated into cloud IaaS and platform as a service (PaaS) providers' service offerings by experimenting with process and workflow changes that accommodate the incorporation of containers.
- Avoid using upstream open source (e.g., Kubernetes) directly unless the organization has adequate in-house expertise to support.

Sample Vendors

Alibaba Cloud; Amazon Web Services; Google; IBM; Microsoft; Mirantis; Red Hat; SUSE; VMware

Gartner Recommended Reading

Market Guide for Container Management

Hyperautomation

Analysis By: Frances Karamouzis, Keith Guttridge, Laurie Shotton, Saikat Ray

Benefit Rating: Transformational

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Business-driven hyperautomation is a disciplined approach that organizations use to rapidly identify, vet, and automate as many business and IT processes as possible. Hyperautomation involves the orchestrated use of multiple technologies, tools or platforms to achieve business results. These include, but are not limited to, AI, machine learning, event-driven software architecture, robotic process automation (RPA), iPaaS, packaged software and process/task automation tools.

Why This Is Important

The primary reason that hyperautomation is critical is the unrelenting demand for accelerated growth through business model innovation or disruption, coupled with the underlying foundation of operational excellence across processes and functions. This is important as organizations continue to focus on business outcomes such as higher quality, more resilient processes, and higher usage due to employee- and customer-centric experiences, among others.

Business Impact

The most important business impacts are aligned to business outcomes such as cost optimization, growth, business agility or innovation. Hyperautomation initiatives are fluid enough to align to one or all of these outcomes. Examples of results may be better (higher quality, more resilient) business or IT processes, speed (time to market, cycle time reduction and quicker adoption) or intelligent (data-driven) decision making at scale.

Drivers

- The biggest driver of hyperautomation is funding from business units (as opposed to the IT budget). These business units continue to hire and fund initiatives driven by fusion teams and business technologists.
- The continued unabated spending on hyperautomation initiatives is forecast to exceed $1 trillion in 2023. This includes spending on products (software, platforms and tools) coupled with services spending on consulting, system integration and managed services.
- Additionally, there have been five successive years of capital investment of $1 billion or more in vendors that can be attributed to the various technology categories that enable hyperautomation initiatives.
- The increased investment has fueled the growth of offerings with expanded breadth and depth within the vast vendor landscape (both organic growth and through acquisitions).

Obstacles

- **Lack of measurement of quantifiable value:** Only a few organizations (estimated at less than 20%) have mastered the measurement of hyperautomation initiatives.
- **Lack of planning for total cost of ownership (TCO) or governance:** The explosion of funded hyperautomation initiatives, coupled with the need for speed, often leaves unaddressed the all-important planning for post-production-managed operations and governance structures.
- **“Siloed” approach:** The ubiquity of hyperautomation has led to an incredible volume and velocity of adoption across functions. Unfortunately, the concurrent nature across business functions has been executed via “siloed” or diffuse purchases of technology tools, solutions and platforms.
- **Technology confusion and overspend:** There is no single vendor or technology that will enable hyperautomation initiatives. Highly fragmented and overlapping technology markets have resulted in complex architectures, overspending and lack of enterprise orchestration.

User Recommendations

- Define shared ownership and metrics. Focus on regular intervals for measurement and updates. The leading organizations in the world ensure this involves finance to facilitate public reporting of success.
- Maximize the likelihood of successful hyperautomation initiatives by architecting and planning multiple concurrent initiatives. Demand holistic mapping of collective initiatives, rather than siloes within specific functions.
- Recognize that the technology is not trivial as there is no single vendor or technology that will enable hyperautomation initiative. Focus on modularity and discoverability in the design. Take an API-first approach.
- Ensure appropriate investment in vendor management and risk competencies due to the volume of services and technologies involved.
- Establish and curate an adaptive governance structure with the goal of managing risk, and driving operational resiliency and agility while optimizing TCO.

Sample Vendors

Automation Anywhere; Boomi; Celonis; Microsoft; OutSystems; SnapLogic

Gartner Recommended Reading

The Gartner 2023 Predictions: Hyperautomation (Inclusive of AI, RPA & Low Code)

The Executive Guide to Maximizing Hyperautomation

Future of Work Trends: Hyperautomation Growth Initiatives Delivered by High-Performance Fusion Teams

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

Vulnerability Prioritization Technology

Analysis By: Mitchell Schneider, Craig Lawson

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Vulnerability prioritization technology (VPT) streamlines a range of vulnerability telemetry sources into a single location — using intelligence sources, analytics and visualizations and to efficiently provide prioritized, pragmatic recommendations on how best to perform critical remediation/mitigation activities. The approach considers the exploitability of a vulnerability, asset or business-criticality, the severity of a vulnerability and compensating controls in place.

Why This Is Important

VPT supports a risk-based vulnerability management (RBVM) approach. These products and services provide a consolidated view of exposures by leveraging the telemetry from sources, including vulnerability assessment (VA) tools, configuration management databases (CMDBs), endpoint detection and response (EDR), penetration testing results and application security testing (AST). VPT adds intelligence and efficiency by leveraging analytics and various threat and vulnerability intelligence sources.

Business Impact

VPT is a form of automation that leverages data science, advanced analytics and vulnerability intelligence to improve VA and prioritization, and rapidly identify the highest-risk exposures for remediation. Moreover, VPT provides the ability to track the VM life cycle via a centralized view. The increase of security incidents and breaches drives many organizations to adopt VPT solutions to implement an effective VM program. This has also caused VA vendors to align more to the RBVM methodology.

Drivers

- Organizations are inundated with vulnerability findings prioritized solely by Common Vulnerability Scoring System (CVSS) scores. VPT solutions contextualize these findings with active threat information, resulting in increased actionability. For example, a vulnerability that is a low risk today might be a high-impact vulnerability tomorrow due to the dynamic changes driven by attackers, while the CVSS score would remain relatively static.

- Interest in the VPT market has accelerated within the last 12 months, according to Gartner research and client inquiries. VPT identifies more pragmatic risks to the organization and helps prioritize actions for vulnerability treatment — whether via remediation (e.g., patching) and/or compensating controls (e.g., intrusion prevention system [IPS] and web application firewalls [WAFs]) — to avoid potential compromise or beginnings of a breach.

- VPT can provide savings in terms of operational full-time employee (FTE) costs due to the automation of vulnerability prioritization, which facilitates attack surface reduction efforts, and results in improved continuity of operations. This is especially beneficial for organizations looking to retain talent by focusing them on more value-added activities.

- The need to take more proactive security actions is offered through other forms of vulnerability prioritization, such as attack path mapping. Attack path mapping is understanding if and how the attacker targets your organization, and what path they could potentially take to get in — uncovering paths to high value assets and contextualizing vulnerabilities risks.

Obstacles

- VPT solutions require a more mature vulnerability management program to be effective. If there are broken processes in the exposure management program, the value of VPT will be limited.

- Organizations that are fixated on CVSS severity as the defining characteristic of how serious a vulnerability is will not be able to get full value from VPT approaches since that metric-driven output is rarely based on risk — as factors like threat activity, asset context and existing security controls are not considered.

- There are overlapping capabilities between VPT and cyber asset attack surface management (CAASM), leading to buyer confusion. CAASM is focused on aggregation of data and visibility, while VPT is focused on improving an organization's RBVM operational processes.

- Attack path mapping is an output of vulnerability prioritization and breach and attack simulation (BAS) to support cybersecurity validation initiatives, but is different from testing security controls. Your organization may already have this capability via another tool.

User Recommendations

- Implement a risk-based approach that correlates asset value and business impact to calculate a risk rating, and automate this through a VPT.

- Augment VA tools with stand-alone VPT solutions for better prioritization, or use existing VPT capabilities that assist with the effective methodology for real risk reduction. This enables vendor consolidation and places less effort on new training and tool deployment.

- Identify vendors with patching and SOAR integrations. This puts the security team in control of workflows. Evaluate if this approach is appropriate. If so, leverage remediation workflow automation and avoid using two different tools.

- Deploy VPT that takes into account the presence (and configuration) of existing security controls to enhance prioritization efforts. This capability is increasing across the market.

- Identify vendors with CAASM capabilities, or who have connectors with your CAASM to better integrate the two products to solve both visibility and improve operational processes.

Sample Vendors

Brinqa; Cisco; Flashpoint; HivePro; Ivanti; NopSec; NorthStar; Nucleus Security; ServiceNow; Skybox Security

Gartner Recommended Reading

How To Implement a Risk-Based Vulnerability Management Methodology

Tracking the Right Vulnerability Management Metrics

Quick Answer: What Are the Top and Niche Use Cases for Breach and Attack Simulation Technology?

Innovation Insight for Attack Surface Management

Composable Infrastructure

Analysis By: Tony Harvey, Paul Delory, Philip Dawson

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Composable infrastructure uses an API to create physical systems from shared pools of resources. The implementation connects disaggregated banks of processors, memory, storage devices and other resources by a hardware fabric. However, composable infrastructure software can also aggregate or subdivide resources in traditional servers or storage.

Why This Is Important

Servers, storage and fabrics are traditionally deployed as discrete products with predefined capacities. Individual devices, or resources, are connected manually and dedicated to specific applications, making the system inflexible and expensive to change and scale. Composable infrastructure replaces this with a pool of components that can be dynamically assigned as needed, increasing agility, easing capacity planning and reducing costs.

Business Impact

Stranded hardware resources that are underutilized represent significant costs in IT. The composable infrastructure enables hardware resources to be aggregated from a pool of components via APIs to dynamically match the infrastructure to the needs of the workload. This increases component utilization, reduces hardware overprovisioning, decreases costs, and improves IT responsiveness to the business's requirements.

Drivers

- Compute Express Link (CXL) provides the necessary capabilities to disaggregate and pool memory and I/O as well as providing a standardized set of APIs to manage the disaggregated hardware.
- Hyperscale cloud vendors are moving toward composable designs utilizing CXL to increase hardware utilization and reduce the costs of stranded hardware.
- Test and development environments benefit from composability, where infrastructure with varying characteristics must be repeatedly deployed, deconstructed and redeployed.
- Multitenant environments benefit from composable infrastructure by allowing a pool of hardware to be dynamically configured, assigned, reconfigured and reassigned based on tenant requirements.

Obstacles

- Current composable implementations are limited in that pooled resources are restricted to using hardware from a single vendor.
- Existing composable infrastructures are limited to just composing storage and I/O, limiting the use cases.
- A proliferation of vendor-specific APIs and a lack of off-the-shelf software for managing composable systems are also headwinds to widespread adoption.

User Recommendations

- Deploy composable infrastructure when the workload or use case demands that infrastructure must be resized and administered frequently or when composability increases the use of packaged standardized high-cost components.
- Replace existing infrastructure to obtain composable infrastructure only if you have sufficiently mature automation tools and skills to implement composable features and yield financial or business benefits.
- Verify that your infrastructure management software supports composable system APIs or that you have the resources and skill sets to write your own management tools.

Sample Vendors

Cisco; Dell Technologies; GigaIO; Hewlett Packard Enterprise; Intel; Liqid; Western Digital

Gartner Recommended Reading

Market Guide for Servers

Emerging Tech: Compute Express Link Redefines Server Memory Architectures

Emerging Tech Impact Radar: Compute and Storage

2022 Strategic Roadmap for Compute Infrastructure

ARO

Analysis By: Daniel Betts

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Application release orchestration (ARO) combines deployment automation, pipeline and environment management with release orchestration capabilities to simultaneously improve the quality, velocity and governance of application releases. ARO enables organizations to automate and scale release activities across multiple diverse teams (e.g., DevOps), technologies, development methodologies (e.g., agile), delivery patterns (e.g., continuous), pipelines, processes and toolchains.

Why This Is Important

Demand is growing and will continue to grow, for new applications and features delivered faster to support business agility. The resulting tumultuous and transformative activity (often in the form of DevOps/DevSecOps initiatives) has created multiple buyers for ARO capabilities. These buyers often desperately need ARO's cohesive value, yet are challenged to articulate and/or gain consensus around the business criticality of release activities to drive adoption.

Business Impact

ARO tools provide increased transparency in the release management process by making bottlenecks and wait for states visible in areas such as infrastructure provisioning or configuration management. Once these constraints are visible and quantifiable, business value decisions can be made to address them and measure improvement. This speeds the realization of direct business value, as new applications and enhancements/bug fixes can be more quickly and reliably delivered.

Drivers

- Agility and productivity gains: Faster delivery of new applications and updates in response to changing market demands.

- Cost reduction: Significant reduction of manual interactions by high-skill and high-cost staff, freeing them to work on higher-value activities.

- Risk mitigation: Consistent use of standardized, documented processes and configurations across multiple technology domains.

- Improvement and remediation: Use of dashboard views over metrics outlining and predicting release quality and throughput.

- Improved visibility and traceability into the release process.

Obstacles

- The need to map capabilities to the client's internal delivery challenges or opportunities.
- Vendors in the DevOps toolchain market are building ARO features into platform solutions, with ARO as a subset of capabilities that can hide their value.
- Challenges in capturing the release orchestration space, due to maturity (feature parity across supplier platforms) in the market.

User Recommendations

- Organize activities into three categories: deployment automation, pipeline and environment management, and release orchestration.
- Explore DevOps platforms that provide ARO along with other native capabilities.
- Prioritize capabilities for current and future needs prior to evaluating vendors. When evaluating ARO tools for selection, prioritize tool features and map capabilities to requirements. Where legacy environments exist, those should be weighted more heavily.
- Simplify and speed up the transition to automated workflows by documenting current application release procedures, activities and artifacts performed by both traditional and DevOps teams.
- Confirm the availability of an ARO platform dashboard, with release performance and underlying platform metrics.

Sample Vendors

CloudBees; Digital.ai; GitLab; Harness; Microsoft; Plutora

Gartner Recommended Reading

Market Guide for Value Stream Delivery Platforms

Market Guide for Value Stream Management Platforms

How to Build and Evolve Your DevOps Toolchains

Beware the DevOps Toolchain Debt Collector

Intent-Based Networking

Analysis By: Andrew Lerner

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

The IETF defines intent-based networking (IBN) as a set of operational goals and outcomes defined in a declarative manner without specifying how to achieve or implement them. Gartner further specifies IBN as a closed-loop system to design, provision and operate a network based on business policies. IBNs translate business policies to network configurations, automate network activities, maintain an awareness of network health and provide continuous network assurance and dynamic optimization.

Why This Is Important

Intent-based networks simultaneously improve network agility and reliability while enabling a common policy across multiple infrastructures. Unfortunately, the term is used loosely by network vendors. Thus, most offerings marketed as intent-based fall short of the complete functionalities of intent-based networking. Instead, we observe an incremental adoption of the subcomponents of an IBN, including network automation, configuration validation and network assurance.

Business Impact

A complete IBN implementation can reduce the time taken to deliver network infrastructure to business leaders by an estimated 50% to 90%. It can simultaneously reduce the number and duration of outages by an approximate 50%. However, there has been limited impact to date due to low real-world adoption and a lack of viable, easy-to-use full IBN products.

Drivers

- There is a desire to make networks more agile in conjunction with cloud deployments and digital business.
- Intent-based networking offers a reduced operating expenditure (opex) associated with managing networks. Therefore, more senior-level network resources are free to focus on more important strategic tasks.
- There is a desire to simplify network administration amid the increasing complexity of networking with overlays, cloud environments and containers.
- IBN allows real-time self-documentation, which also includes the rationale — that is, the intent behind design or configuration decisions.
- IBN can lead to improved compliance and simplified auditing. This is due to the algorithmic correctness of configurations that provide self-validation, direct mapping to the business intent and ongoing, dynamic and real-time validation.
- IBN can help to reduce the impact of enterprises that are not able to hire or retain senior-level network engineers and architects.
- In October 2022, the IETF published the informational document, RFC9315, which helps to streamline IBN terminology and definition. This research document can reduce confusion, foster consistency and consequently clear hurdles to adoption.

Obstacles

- Only a limited number of vendors offer complete IBN capabilities. Very few offerings translate a higher-level intent into network configuration — we estimate that there are fewer than 1,000 full deployments.
- Network automation, AI networking and AIOps all deliver some of the value intent-based networks offer, and are often simpler to implement. This limits, prevents or delays IBN.
- Vendors are increasingly delivering recommendation engines and predictive capabilities in their management products, which limits or delays IBN.
- Very few vendors provide full intent-based networks. Instead, vendors release products that deliver some discrete individual benefits, often with limited integration between them.
- Full IBN is restricted to greenfield or very homogeneous environments that are deployed in a very prescriptive, structured and specific way. This inflexibility limits adoption.
- It is challenging to define intent for preexisting network deployments.

User Recommendations

- Tune out vendor marketing of products listed as “intent-based” or “intent-driven.” Instead, invest in products that enable network automation and provide network assurance or prescriptive predictions with specific recommendations.
- Invest in network products that provide specific and actionable recommendations down to the device and configuration level when purchasing equipment and tooling solutions. The combination of these investments can help to enable closed-loop automation and operations.

Sample Vendors

Gluware; Juniper Networks; NetBrain

Gartner Recommended Reading

Market Guide for Network Automation Tools

Climbing the Slope

Hybrid Cloud Computing

Analysis By: David Smith, Milind Govekar

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Hybrid cloud computing comprises two or more public and private cloud services that operate as separate entities but are integrated. A hybrid cloud computing service is automated, scalable and elastic. It has self-service interfaces and is delivered as a shared service using internet technologies. Hybrid cloud computing needs integration between the internal and external environments at the data, process, management or security layers.

Why This Is Important

Hybrid cloud theoretically offers enterprises the best of both worlds — cost optimization, agility, flexibility, scalability and elasticity benefits of public cloud, in conjunction with control, compliance, security and reliability of private cloud (assuming their on-premises environments are truly cloud). As a result, virtually all enterprises have the desire to augment internal IT systems with external cloud services. Note that many organizations start with hybrid IT, which lessens the requirement of a true private cloud.

Business Impact

Hybrid cloud computing enables an enterprise to leverage both its data centers as well as the capabilities of the public cloud. It is transformational because changing business requirements drive the optimum use of private and/or public cloud resources. This approach improves the economic model and agility and sets the stage for new ways for enterprises to work with suppliers, partners (B2B) and customers (B2C).

Drivers

- The desire to evolve data centers to become more cloudlike and, therefore, have a private cloud having cost and other characteristics more like a public cloud, while maintaining “in house” infrastructure for key privacy, security, data residency or latency needs.

- As more providers deliver hybrid cloud offerings, they increasingly deliver a packaging of the concept. “Packaged hybrid” (a flavor of distributed cloud) means that you have a vendor-provided private cloud offering that is packaged and connected to a public cloud in a tethered way. Azure Stack HCI from Microsoft is a good example of this packaging, but there is another approach as well. We call these two main approaches “like for like” hybrid and “layered technology” hybrid (spanning different technology bases). Packaged hybrid cloud is a key component of the distributed cloud concept.

- The solutions that the hybrid cloud provides include service integration, availability/disaster recovery, cross-service security, policy-based workload placement and runtime optimization, as well as cloud service composition and dynamic execution (for example, cloud bursting).

Obstacles

- Hybrid cloud computing is different from multicloud computing, which is the use of cloud services from cloud providers for the same general class of IT service.

- Hybrid cloud computing complements multicloud computing. Although most organizations are integrating applications and services across service boundaries, few large enterprises implemented hybrid cloud computing for a few services.

- Hybrid cloud is different from hybrid IT, where IT organizations act as service brokers as part of a broader IT strategy and may use hybrid cloud computing. Hybrid IT can also be enabled by service providers focused on delivering cloud service brokerage, multisourcing, service integration and management capabilities. These services are provided by vendors, such as Accenture, Wipro and Tata Consultancy Services (TCS), and other service providers and systems integrators.

User Recommendations

- Note that internally run, virtualized environments are often recast as “private clouds,” then integrated with a public cloud environment and called a “hybrid cloud.” Hybrid cloud assumes that the internal environment is truly a private cloud. Otherwise, the environment is hybrid IT.

- Establish security, management, and governance guidelines and standards when using hybrid cloud computing services to coordinate the use of these services with public and private services.

- Approach sophisticated cloud bursting and dynamic execution cautiously, because these are the least mature and most problematic hybrid approaches.
- Create guidelines/policies on the appropriate use of the different hybrid cloud models to encourage experimentation and cost savings, and to prevent inappropriately risky implementations.
- Coordinate hybrid cloud services with noncloud applications and infrastructure to support a hybrid IT model.

Gartner Recommended Reading

Top Strategic Technology Trends for 2021: Distributed Cloud

‘Distributed Cloud’ Fixes What ‘Hybrid Cloud’ Breaks

Predicts 2023: The Continuous Rising Tide of Cloud Lifts All Boats

Leverage Platform Engineering to Scale DevOps Platforms Into Hybrid Cloud

Immutable Infrastructure

Analysis By: Neil MacDonald, Tony Harvey

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Immutable infrastructure is a process pattern (not a technology) in which the system and application infrastructure, once deployed, are never updated in place. Instead, when changes are required, the infrastructure and applications are simply updated and redeployed through the CI/CD pipeline.

Why This Is Important

Immutable infrastructure ensures the system and application environment, once deployed, remains in a predictable, known-good-configuration state. It simplifies change management, supports faster and safer upgrades, reduces operational errors, improves security, and simplifies troubleshooting. It also enables rapid replication of environments for disaster recovery, geographic redundancy or testing. This approach is easier to adopt with cloud-native applications.

Business Impact

Taking an immutable approach to workload and application management simplifies automated problem resolution by reducing the options for corrective action to, essentially, just one — repair the application or image in the development pipeline and rerelease. The result is an improved security posture and a reduced attack surface with fewer vulnerabilities and a faster time to remediate when new issues are identified.

Drivers

- Linux containers and Kubernetes are being widely adopted. Containers improve the practicality of implementing immutable infrastructure due to their lightweight nature, which supports rapid deployment and replacement.

- The GitOps deployment pattern, which emphasizes continuously synchronizing the running state to the software repository, has become an effective way to implement immutable infrastructure in Kubernetes-based, containerized environments.

- Infrastructure as code (IaC) tools (including first-party cloud provider IaC tools) have increasingly integrated configuration drift detection and correction, improving the practicality of implementing immutable infrastructure across an application's entire stack and environment.

- Interest in zero-trust and other advanced security postures where immutable infrastructure can be used to proactively regenerate workloads in production from a known good state (assuming compromise), a concept referred to as "systematic workload reprovisioning."

- For cloud-native application development projects, immutable infrastructure simplifies change management, supports faster and safer upgrades, reduces operational errors, improves security, and simplifies troubleshooting.

Obstacles

- The use of immutable infrastructure requires a strict operational discipline that many organizations haven't yet achieved, or have achieved for only a subset of applications.
- IT administrators are reluctant to give up the ability to directly modify or patch runtime systems.
- Applying the immutable infrastructure pattern is most easily done for stateless components. Stateful components, especially data stores, represent special cases that must be handled with care.
- Implementing immutable infrastructure requires a mature automation framework, up-to-date blueprints and bills of materials, and confidence in your ability to arbitrarily recreate components without negative effects on user experience or loss of state.
- Many enterprise applications are stateful applications deployed on virtual machines. These applications are oftentimes commercial off-the-shelf and are not designed for fully automated installation when redeployed.

User Recommendations

- Reduce or eliminate configuration drift by establishing a policy that no software, including the OS, is ever patched in production. Updates must be made to individual components, versioned in a source-code-control repository, then redeployed.
- Prevent unauthorized change by turning off all administrative access to production compute resources. Examples of this might include not permitting Secure Shell or Remote Desktop Protocol access.
- Adopt immutable infrastructure principles with cloud-native applications first. Cloud-native workloads are more suitable than traditional on-premises workloads.
- Treat scripts, recipes and other codes used for infrastructure automation similar to the application source code itself, as this mandates good software engineering discipline.
- Include immutable infrastructure scripts, recipes, codes and images in your backup and ransomware recovery plans as they will be your primary source to rebuild your infrastructure after an infection.

Sample Vendors

Amazon Web Services; Google; HashiCorp; Microsoft; Perforce; Progress; Red Hat; Snyk; Turbot; VMware

Gartner Recommended Reading

Comparing DevOps Architecture to Automate Infrastructure and Operations for Software Development

2022 Strategic Roadmap for Compute Infrastructure

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

Innovation Insight for Continuous Infrastructure Automation

Market Guide for Cloud-Native Application Protection Platforms

Continuous Delivery

Analysis By: Hassan Ennaciri

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Continuous delivery (CD) is a software engineering approach that enables teams to build critical software quickly, while ensuring the software can be released reliably anytime. Through dependable, low-risk releases, CD allows continuous adaptation of the software to incorporate user feedback, market shifts and business strategy changes. This approach requires the engineering discipline to facilitate complete automation of the software delivery pipeline.

Why This Is Important

The growing success of DevOps initiatives continues to drive investments in CD capabilities. CD improves software release velocity and reliability, while simplifying compliance enforcement via automation. It is a prerequisite and the first step to continuous software deployments for organizations that aspire to push changes with zero downtime.

Business Impact

CD is a key practice for a DevOps initiative as it reduces the build-to-production cycle time. As a result, it accelerates the positive impact of new applications, functions, features and fixes by increasing velocity across the application life cycle. The positive impacts include improved business delivery and end-user satisfaction, improved business performance and agility, and risk mitigation via rapid delivery of updates.

Drivers

- Increased adoption of Agile and DevOps practices to deliver solutions.
- Pressure from digital business to improve release velocity and reliability.
- Additional compliance requirements that require automation and orchestration of release activities for better traceability and auditability.
- The need to improve delivery outcomes to deploy application builds and updates more consistently, by extending the benefits of continuous integration (CI) and automated testing to continuously build deployable software.

Obstacles

- Organizational culture and collaboration between teams with different roles and skills are major barriers to CD success. Agile practices that helped bridge the gap between business and development must be extended to deployment, environment configuration, monitoring, and support activities.
- Lack of value stream mapping of product delivery hinders visibility and quick feedback loops for continuous improvements. Teams struggle to improve and focus on value work, as they don't have insights into the critical steps in the process, the time each step takes, handoffs, and wait states.
- Manual steps and processes involved in deploying to production environments impact software flow delivery.
- Other challenges impacting the success of CD include application architecture, lack of automation in all areas of testing, environment provisioning, configuration security and compliance.

User Recommendations

- Evaluate all associated technologies when you start a CD initiative and take an iterative approach to adoption. This will require collaboration with different stakeholders from the product, development, security and operations teams.
- Establish consistency across application environments for a higher likelihood of success and implement a continuous improvement process that relies on value stream metrics.
- Evaluate and invest in associated tooling, such as application release orchestration tools, containers, and infrastructure automation tools. These tools provide some degree of environment modeling and management, which can prove invaluable for scaling CD capabilities across multiple applications.
- Explore a DevOps platform that provides fully integrated capabilities and enables continuous delivery of software.

Sample Vendors

Broadcom; CloudBees; GitLab; Harness; JFrog; Red Hat

Gartner Recommended Reading

How to Build and Evolve Your DevOps Toolchains

Market Guide for Value Stream Management Platforms

Beware the DevOps Toolchain Debt Collector

Network Automation

Analysis By: Andrew Lerner

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Network automation tools help to automate provisioning/configuration, troubleshooting, operations/maintenance, validation, and reporting of network components. Network automation tools typically interact with routers, switches, firewalls, application delivery controllers, service provider components (WAN circuits) and cloud provider services (VPCs and load balancers, for example). Network automation tools are delivered as software and may support one or more vendors.

Why This Is Important

Network automation tools improve agility and efficiency, lower costs, and reduce errors. Network automation adoption in the enterprise lags that of server automation, as more than 65% of enterprise networking activities are performed manually. Limited network automation creates avoidable bottlenecks in provisioning, and in incident resolution, while increasing the likelihood of human errors.

Business Impact

Network automation tools drive positive business outcomes by improving service delivery, availability, management efficiency, staffing efficiency and compliance activities.

Drivers

- Digital businesses demand increased network agility to quickly adapt to changing needs, such as connecting to customers, partners, cloud, delivering servers or restoring service during an incident.
- Agile software development, DevOps practices, infrastructure as code (IaC) and GitOps initiatives all mandate increased network automation.
- The traditional approach of manually updating each device is too slow, fraught with danger from typos and missed devices, increases outage likelihood, and is expensive due to increased personnel time. Network automation tools allow organizations to make network changes across tens, hundreds, thousands or more devices in short periods of time.
- Growing automation in other infrastructure domains, such as server and cloud, increases the desire for network automation.
- Automation helps to reduce manual network configuration, often to deliver capabilities to the business faster, or to reduce repetitive tasks to increase staff efficiency.
- It helps fulfill the desire to increase device configuration accuracy to help with auditing, troubleshooting and/or reducing manual errors.
- Network vendors are increasingly embedding automation capabilities in their products.

Obstacles

- Rigid enterprise change management policies.
- A culture of aversion to risk due to the potential impact of an outage.
- Technical debt in the form of heterogeneous and complex environments, including vendors, devices and configuration.
- Inconsistent or undocumented workflows related to network activities.
- Limited time and/or limited clear incentives for personnel to acquire network automation skills and automate manual activities.
- Limited budget, as the benefits of really good automation tools (vs. mediocre) are apparent at the practitioner level, but can be very difficult to justify the upstream investment.
- Limited software skill sets needed in network automation, such as Python or development processes.
- Fragmented market for network automation tools, which results in many organizations having multiple tools, limiting efficiency.

User Recommendations

- Start with small network initiatives and iterate by focusing on nonchange and/or nonproduction activities first.
- Derive quick “wins” by initially automating simple activities such as troubleshooting, baselining performance levels, and configuration and state archiving.
- Invest in personnel by shifting hiring and training focus toward specific software competencies, including Ansible and Python, community forums, and by cross-pollinating networking teams with adjacent DevOps personnel.
- Measure, reward and socialize network automation by introducing team and individual goals that target business outcomes, such as faster service delivery, improved application availability or reduced opex.

Sample Vendors

Gluware; HashiCorp; Itential; Network to Code; Red Hat; SolarWinds

Gartner Recommended Reading

Market Guide for Network Automation Tools

Software-Defined Infrastructure

Analysis By: Philip Dawson

Benefit Rating: Low

Market Penetration: 20% to 50% of target audience

Maturity: Obsolete

Definition:

Software-defined infrastructure (SDI) enables abstraction of the physical infrastructure, with its services exposed via APIs enabling greater levels of automation, policy-based orchestration and reuse. SDI includes software-defined data center, network, storage, compute and SD edge infrastructure.

Why This Is Important

Software-defined is the further abstraction of software from hardware. It enables businesses to be more agile and flexible by enabling programmatic control of the infrastructure through software interfaces. SDI combines compute (SDC), network (SDN) and storage (SDS), but SDI also extends to non-data-center infrastructure, with the use of either software-defined monitoring devices or machines.

Business Impact

While data center SDI is embedded in other data center initiatives, such as cloud and hyperconverged infrastructure, SDI is now focused on key verticals operating in multiple edge locations, such as retail, manufacturing, retail banking, distribution and utilities. It also continues to extend Internet of Things (IoT), non-data-center SDI and SDS storage initiatives for new IT and software-defined WAN (SD-WAN) operations and functions.

Drivers

- SDI data center infrastructure is well-covered with compute (SDC), network (SDN, now obsolete), edge (SD-WAN), and storage (SDS), but SDI also extends to non-data-center infrastructure with the use of monitoring devices or machines that are software-defined.
- SDI reaches beyond and between software-defined data centers (SDDCs), leveraging SDI benefits and features for new multimode applications and edge and/or IoT endpoints.
- In 2023, SDI's continued presence of hype is enabled through the use of sensors and adapters that are abstracted through software, stretching SDI to the edge, IoT and operational technology (such as retail point of sale [POS]), rather than traditional, IT-driven SDI through a data center or cloud.
- Key verticals operating in multiple, geographically distributed locations, such as retail, manufacturing, retail banking, distribution and utilities, are extending IoT and non-data-center SDI initiatives for new edge and IoT operations and functions.

Obstacles

- SDI is now tied to extending data center vendor technology, not interoperability.
- SDI overlaps other integrated systems taxonomy, like hyperconvergence, as it drives cloud to data center and edge adoption.
- SDI continues releasing vendor-specific silo technology (not heterogeneous and service-driven) and, hence, it continues to be obsolete as multivendor interoperability standards and technology silos persist, limiting SDI integration between vendors.
- SD-WAN segmentation is driving SDI to the edge and is architecturally different from SDN, which is focused more on data center infrastructure convergence.

User Recommendations

- Include the integration and measurement of non-data-center edge infrastructure, as SDI initiatives roll out tied to SD-WAN and edge initiatives.
- Focus on core IT SDI for compute, network, storage and facilities, but expand the impact of SDI on IoT, edge computing, remote office/branch office (ROBO) and other operational technologies.
- Anticipate SDI to be tied to a specific vendor or technology silo, such as SDS storage and SD-WAN network hardware or virtualization software. Be cautious not to commit to a vendor's SDI without realizing the specific area of lock-in.

Sample Vendors

IBM (Red Hat); Intel; Microsoft; VMware; Wipro Enterprises

Gartner Recommended Reading

Predicts 2023: XaaS Is Transforming Data Center Infrastructure

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

SOAP

Analysis By: Chris Saunderson

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

A service orchestration and automation platform (SOAP) enables foundational workload automation and support for event-driven business models and cloud infrastructure. Organizations must deliver service orchestration and automation to drive customer-focused agility as a part of cloud, big data and DevOps initiatives.

Why This Is Important

The capabilities of workload and workflow automation platforms are foundational to meeting increased business agility demands. SOAP enables efficient management of scheduled tasks, and also extends to event- and integration-driven architectures. Delivery across new topologies (edge and cloud), and meeting new workload demands, requires evaluating and modernizing practices and tooling related to business processes delivered.

Business Impact

Digital ecosystems expanding across an increasingly complex workload topology require a rethinking of the ways in which those business processes are enabled and executed. Continued cost and skilled staff pressures are leading to reevaluation of current capabilities and driving investment into cost-optimized or supportable capabilities. Therefore, organizations looking to modernize their workload automation capabilities should add SOAP to their technology roadmap.

Drivers

- The foundation of workload automation is no longer sufficient to meet the needs of new and evolving business demands. An evolution to service orchestration is required to meet both the business process execution expectations of the organization, and to enable new opportunities. This is magnified with the need for increased visibility, auditability and transparency to meet security and compliance requirements.

- The expansion of workload locations to the edge, colocation as well as on-premises and cloud have exposed challenges in both the capabilities of existing platforms and the cost and availability challenges associated with expansion. Similarly, the increase in demand for support of data and analytics requirements by the infrastructure and operations (I&O) team further demonstrates the need for modernization.

- DevOps initiatives require modernization of workload automation to support iterative definition of jobs-as-code, which is challenging for traditional workload tools.

- The expansion of business technologist roles demands self-service access to create business automation workflows, via democratization and low-code interfaces.

- There are limitations in existing tooling, surfaced by hybrid execution topologies.

- Organizations are increasingly evaluating SaaS-first deployment requirements to address the overall cost of using these types of platforms, displacing I&O costs by adopting SaaS.

Obstacles

- Foundational capabilities are difficult to displace, as process execution efficiency and stability are table stakes.
- Reliability is delivered by existing solutions. Disruption due to migration between suppliers is perceived as complex and time-consuming, risking this reliability.
- The adoption of SaaS platforms is seen as risky from compliance, complexity and availability perspectives.
- It is difficult to find and retain skilled resources to sustain existing platforms and implement new ones.
- There have been a number of SOAP vendor changes — notably consolidation of suppliers of these solutions, and cost and licensing changes. This is forcing evaluation of the market and alternative suppliers.

User Recommendations

- Ensure that a full catalog of business processes being executed through traditional workload automation or workflow automation platforms is cataloged and maintained.
- Align SOAP services to new or evolving business demands by integrating edge workloads, cloud-native services or event-driven architectures into the services offered by the platform.
- Assess organizational SaaS posture to shape supplier evaluation criteria.
- Utilize licensing changes as a catalyst to evaluate and reevaluate suppliers in the SOAP market.
- Evaluate SOAP integrations with key business systems (e.g., ERP, SaaS and continuous integration/continuous deployment [CI/CD]).
- Source vendors that provide migration implementation, tools and services to speed deployment.

Sample Vendors

ActiveEon; BMC Software; Broadcom; HCLSoftware; InfiniteDATA, PagerDuty; Redwood Software; Resolve Systems; ServiceNow; Stonebranch

Gartner Recommended Reading

Market Guide for Service Orchestration and Automation Platforms

Quick Answer: What Does Redwood Software's Acquisition of Tidal Software Mean for Tidal Automation Customers?

Beware the DevOps Toolchain Debt Collector

Beyond RPA: Build Your Hyperautomation Technology Portfolio

Automated Incident Response

Analysis By: Pankaj Prasad, Padraig Byrne

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Automated incident response (AIR) centralizes alert or incident routing through a policy or rule-based engine, on-call scheduler and streamlined collaboration. AIR solution capabilities improve operational efficiencies with action-oriented insights, shorter incident durations and automated workflows for event routing, easier collaboration, remediation and escalations.

Why This Is Important

Manual processes for incident resolution is a challenge, especially when multiple experts need to be involved, time is of essence and the organization wants to improve efficiency. For DevOps teams, the juggling of contact lists and lack of seamless collaboration inhibit speedy delivery of application features, as well as the stability of features after the release. AIR solutions solve this by automating most of the incident response process and collaboration, and enabling iterative improvement.

Business Impact

AIR solutions deliver value through:

- Automated incident communication to the relevant recipient and visibility across the organization.
- Quick incident resolution minimizing customer impact.
- A well-integrated incident management practice that meets DevOps requirements.
- Insights into incidents and their responses, which helps improve process and operational efficiency.
- Automated workflows that eliminate fatigue and human errors and reduce the turnaround time.

Drivers

- **Incident communication and visibility challenges:** With geographically distributed teams, remote workforce, complex on-call schedules and notification channel preferences, incident triage teams often have difficulty engaging responders quickly. Incident communication itself may lack all the relevant inputs or rely on multiple sources of incident data.
- **Automation of incident response processes:** AIR reduces mean time to acknowledge (MTTA) by automating the process of identifying and contacting the relevant domain experts, and speeds up the resolution process.
- **DevOps and site reliability engineer (SRE) requirements:** Traditional incident management models cannot meet the needs of agile cultures because of manual tasks in the incident response workflow. AIR caters to the need for seamless collaboration across various groups enabling DevOps to underpin its offerings with an effective, consistent IT service management (ITSM) practice.
- **Transparent review and analysis:** AIR tools capture an incident's progress from identification through resolution, including the handoffs needed across various teams. This includes the time and action taken at each step of the incident, and provides vital information for postincident review (PIR) and process review for further enhancements.
- **Workflow automation:** These tools can automate workflows that are part of processes like creating incidents for actionable alerts, opening a communications channel in instant messengers for collaboration, updating on a web-portal and one-click remediation for existing runbooks.

Obstacles

- **Overlapping capabilities:** Although AIR solutions offer differentiating features, they also overlap with ITSM and event management systems, making it difficult to articulate the value of investing in AIR.

- **Service definitions:** Service definitions that connect alerts to responder teams are often challenging to configure as it involves interpretation of a problem based on the notification to identify the domain experts that need to be engaged. Service definitions are also a complex part of AIR onboarding.

- **Portability between solutions:** Migrating from one AIR vendor to another is a reset process, with no defined migration path. The integrations, team and service definitions, responder preferences, and role-based access controls must be reconfigured without sophisticated import/export mechanisms.

- **Maturity in I&O:** Few organizations have the required I&O maturity to quantify impact due to time lost in contacting the right personnel for resolving an issue to justify investing in these tools.

User Recommendations

- Invest in a centralized AIR solution for automating incident management workflows and on-call capability for major incidents and critical events with wide integrations for holistic incident response management.

- Integrate monitoring solutions and service desk systems with bidirectional synchronization to incident response systems, which keeps the incident status synchronized across systems.

- Leverage automation for remediation and to extend incident response capabilities that can integrate with DevOps toolchains.

- Improve incident communication and collaboration by integrating incident workflow processes with ChatOps tools, such as Slack or Microsoft Teams.

Sample Vendors

AlertOps; Atlassian; Derdack; Everbridge; OnPage; PagerDuty; ServiceNow; Splunk

Software Asset Management Tools

Analysis By: Yolanda Harris

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Software asset management (SAM) tools help maintain compliance with software and cloud licensing agreements. They optimize software and cloud spending by identifying opportunities to reuse software, monitor software consumption and provide data to support software negotiations. SAM tools facilitate this by aggregating an organization's entitlement and consumption of data, then reconciling it to establish an effective license position (ELP) and properly govern software use.

Why This Is Important

SAM tools continue to attract interest from organizations across industries. They are designed to simplify the management of complex software licensing (on-premises and SaaS) by discovering, collecting, normalizing and reconciling software consumption with entitlement data to deliver and identify real-time cost and usage optimization opportunities and noncompliance risks. These benefits often extend the use of SAM tools to support security and risk use cases and to manage cloud consumption.

Business Impact

- SAM tools benefit organizations, because managing software and SaaS is a universal challenge that is becoming more difficult with larger software estates, decentralized purchasing, complex licensing and hybrid environments.
- SAM tools help IT and procurement leaders simplify software management by providing a consolidated view of an enterprise software estate. They also support decision making, and the ability to mitigate software risks, optimize software spend and improve life cycle management.

Drivers

- Sourcing, procurement and vendor management (SPVM) leaders often invest in SAM tools to gain visibility into software inventory and usage to improve the enterprise's ability to negotiate with software vendors and proactively manage renewals.

- SAM tools help IT finance and budget owners gain insights into software expenditures for improved forecasting, cost allocation and IT financial management.

- SPVM leaders are under pressure to minimize software costs associated with complex licensing models and increasing usage, as well as to identify unbudgeted compliance fees associated with software vendor audit risks.

- Enterprise architects and IT security teams look to SAM tools to provide visibility into the entire IT estate. They also want to enrich information, such as known vulnerabilities and exposures, end of life, and end of support, which enable enterprises to mitigate risks and plan for upgrades.

- Within infrastructure and operations (I&O), SAM tools have become valuable, because they help consolidate and normalize data from various discovery and inventory sources. This cleansed data can support configuration management database (CMDB) tooling efforts and accelerate time to value for IT service delivery.

- The growing adoption of cloud computing and SaaS has increased the complexity of SAM, with expanding requirements on cloud cost management, complex licensing rules and business-led technology buying.

- The need to manage SaaS software leads to investment in tools that expand the capabilities of traditional SAM tools or replace them with SaaS management platforms (SMPs) and SaaS security tools, which partially address cloud licensing challenges.

Obstacles

- Most sourced software fails to comply with ISO/IEC 19770-3 standards, which supply data and format structures for software publishers to provide entitlement data. This supports automated loading of software entitlements. Due to the lack of adoption, loading entitlements is a resource-intensive process often overlooked when purchasing SAM tools.

- Coupled with complex and hybrid environments, the speed of change often requires manual intervention and SAM managed services providers (MSPs) or additional data collection tools to produce an effective license position (ELP).

- Due to specific use cases and the presence of adjacent tools in their environment that conflict with SAM, organizations often struggle to identify and prove the value of SAM tools.

- Many organizations underestimate the number of direct and indirect resources with specialized skills required to properly use SAM tools for entitlement loading, inventory sources health and data quality checks, or remediation and optimization.

User Recommendations

- Establish a clear, realistic scope by determining which three to five publishers you initially want to manage with your SAM tool. Then, prioritize by compliance risks, spend volume, business-criticality or renewal schedule. Develop a set of use cases the tool must deliver against in managing these publishers, and build on that to add publishers.

- Determine what license metrics, environments — e.g., infrastructure as a service (IaaS) and software as a service (SaaS), — OSs and virtualization technologies are involved with your in-scope publishers. This will help you select appropriate SAM tool(s) for your enterprise.

- Use out-of-the-box integrations with existing inventory sources, where available, and regularly monitor data for accuracy.

- Evaluate SAM MSPs to complement investments in a SAM tool and address tool limitations. Augment resources for tool administrations and operations, such as entitlement loading, ELP creation, and actions to address noncompliance and savings opportunities.

Sample Vendors

Certero; Eracent; Flexera; Matrix42; ServiceNow; Snow Software; USU

Gartner Recommended Reading

4 Keys to Unlock SAM's Strategic Value

The Future of the Software Asset Manager Is About Governance, Not Counting Licenses

Target Software and Cloud Costs by Uniting Software Asset Management and FinOps

Magic Quadrant for Software Asset Management Managed Services

Market Guide for Software Asset Management Tools

How to Select the Right Software Asset Management Tools

Mature Your SAM Discipline by Investing in the Right SAM Tool

Entering the Plateau

Continuous Configuration Automation

Analysis By: Chris Saunderson

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Continuous configuration automation (CCA) tools enable infrastructure administrators and developers to automate the deployment, configuration and operation of systems and software. They support the definition, deployment and maintenance of configuration states and settings. Most CCA tools have an open-source heritage, and most offer commercial support.

Why This Is Important

CCA tools are critical to delivering operational efficiency. They enable automation and DevOps initiatives by deploying and managing infrastructure elements, associated software and configuration changes as code. In combination with infrastructure automation tools, CCA tools form the core of infrastructure-as-code (IaC) capabilities. They also enable the automation of Day 2 operations of deployed systems, expanding their reach into networking, containers, compliance and security use cases.

Business Impact

By enabling automated deployment and configuration of systems, settings and software programmatically, organizations realize:

- **Agility improvements:** CI/CD enablement for infrastructure and operations (I&O) services.
- **Productivity gains:** Repeatable, declarative, version-controlled infrastructure deployment/operation.
- **Cost optimization:** Reductions in manual interventions by skilled staff.
- **Risk mitigation:** Compliance assessment and remediation using standardized processes Improved change success and reliability are also realized.

Drivers

- Organizations need a broader set of deployment and automation functions beyond configuration management, including IaC, patching, application release orchestration (ARO), configuration assessment and auditing (e.g., for regulatory or internal policy compliance) and orchestration of operational tasks.
- CCA provides an automation framework that enables deployment automation and Day 2 operational automation of changes, compliance, and response to incidents or problems.
- CCA tools are essential for I&O administrators to mature from task-based scripting to a more structured approach to automation and delivery.
- There is a need for repeatable, declarative, standardized deployments to be made available to end users or I&O administrators that enable quick delivery of infrastructure to meet end-user needs and I&O policies and baselines.

Obstacles

- Confusion around the capabilities and overlaps of automation tools causing conflict and overinvestment.
- Developers and administrators may use CCA in a silo, further inhibiting enterprisewide adoption.
- IT skill sets hinder the adoption of these tools, requiring source code management and software engineering skills to make full use of capabilities.
- The growing use of IaC tools has created confusion about the role of CCA tools; however, CCA tools are necessary to deliver effective and efficient IaC.

User Recommendations

- Clarify the role that CCA tools fulfill in their toolchain and make selections based on the tasks that are in scope.
- Evaluate the availability of content against organizational use cases. Prioritize CCA tools that provide out-of-the-box content that addresses current pain points and accelerates time to value.
- Include both professional services for enablement and training requirements in cost evaluations. Costs associated with CCA tools extend beyond just the licensing cost.

- Expect to invest in training beyond tool implementation to fully realize the benefits of these tools.
- Guard against developers and administrators reverting to known imperative scripting methods to complete specific tasks in place of using CCA capabilities.
- Maximize the value of CCA tool investments by ensuring that your organization's culture can embrace CCA tools strategically and automate toil (for DevOps and I&O leaders).

Sample Vendors

Inedo; Perforce (Puppet); Progress; Red Hat; Rudder; VMware

Gartner Recommended Reading

Market Guide for Infrastructure Automation Tools

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

Innovation Insight for Continuous Infrastructure Automation

Cloud Migration

Analysis By: Craig Lowery

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Cloud migration is the process of planning and executing the movement of applications or workloads from on-premises infrastructure to external cloud services, or between different external cloud services. At a minimum, applications are rehosted (moved largely as-is to public cloud infrastructure), but are ideally modernized through refactoring or rewriting, or potentially replaced with software as a service (SaaS).

Why This Is Important

Cloud migration is a necessary step for organizations wishing to maximize the business benefits of their use of public cloud computing services. When applications and data in the organization's private data centers are moved into a public cloud, new opportunities are unlocked for the benefit of the business. A structured, well-informed approach to such a move is necessary to avoid negative impacts such as wasted time and investment, or business disruptions.

Business Impact

- The business is able to access the benefits of public cloud without building all of its cloud application portfolio from scratch.
- Existing applications can be migrated into the public cloud and modified to take some advantage of cloud capabilities, yielding near-term cloud-related benefits.
- Cloud migration enables a business to adopt public cloud with the least disruption by evolving organizational structures, operational capabilities and user experiences over time.

Drivers

- Organizations see benefit in public cloud deployments and seek to move all or a portion of their IT data center deployments there to derive positive business impacts.
- Migration allows an organization to leverage existing deployments in their private data centers rather than building everything anew in the cloud.
- Competitors who built their businesses in the cloud or migrated earlier have cloud-based advantages that the organization must counter as quickly as possible. Conversely, getting to the cloud before competitors can give an organization a competitive cloud-based advantage.

Obstacles

- Most organizations lack the tools, expertise and resources to plan and execute a migration. Although some existing tools and skills can be leveraged, they are usually not sufficient to effect a successful migration.
- Organizations often struggle with the new operational aspects of cloud computing, which can result in technically successful migrations that fail to meet business objectives such as improved agility or more efficient IT spending..
- Emphasis on application modernization as part of migration further confuses the market on best practices and strategies.
- Not everything should be moved to the cloud and most organizations will be in a hybrid deployment for some period of time. There are many approaches to achieving a hybrid deployment and organizations may find it difficult to identify, understand and act on their options.

User Recommendations

- Use an external service provider, such as a cloud IT service provider, to improve the chances of a successful migration. Almost all successful large-scale migrations to public cloud infrastructure and platform services (CIPS) are done in conjunction with a service provider. They provide consulting for strategy and planning, tools, and technical staff to implement the move.
- Set a strategy based on business objectives, provide CSP recommended training (badges) for key personnel, and source migration tools from ISVs or the CSP's native toolset if you are an I&O leader electing to perform your own migration.
- Choose the best approach for modernizing an existing application. Although rehosting without modification might be easiest, it brings far fewer benefits than some degree of modernization or outright replacement. Some rehosting migrations are still done for expediency but expectations of cloud-native benefits have become mainstream.

Sample Vendors

Accenture; Deloitte; HCLTech; Infosys; Tata Consultancy Services; Wipro

Gartner Recommended Reading

Magic Quadrant for Public Cloud IT Transformation Services

Critical Capabilities for Public Cloud IT Transformation Services

How to Choose the Right Approach for Application Modernization and Cloud Migration

Decision Point for Choosing a Cloud Migration Strategy for Your Application

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

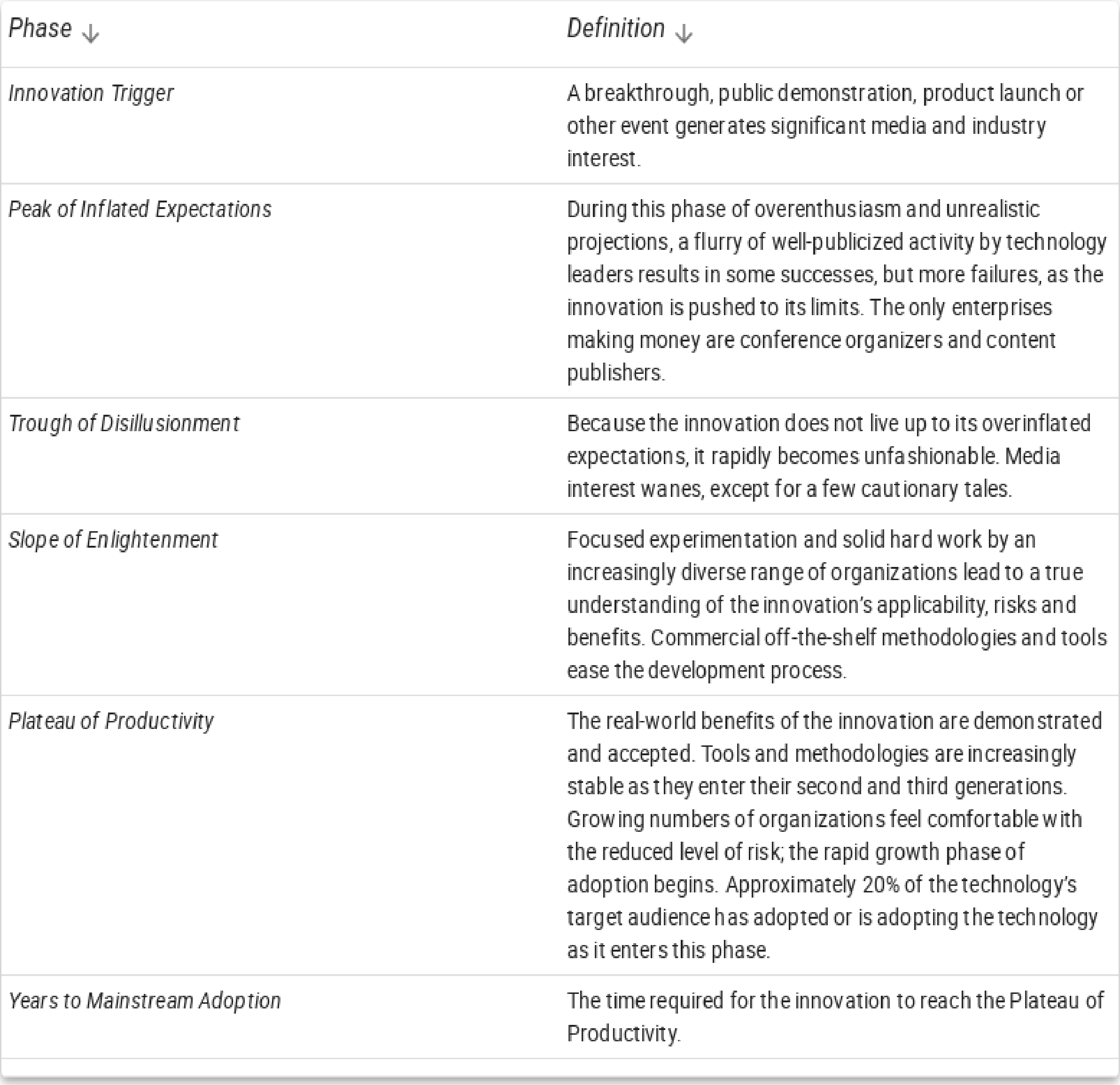
Appendixes

See the previous Hype Cycle: Hype Cycle for I&O Automation, 2022

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)

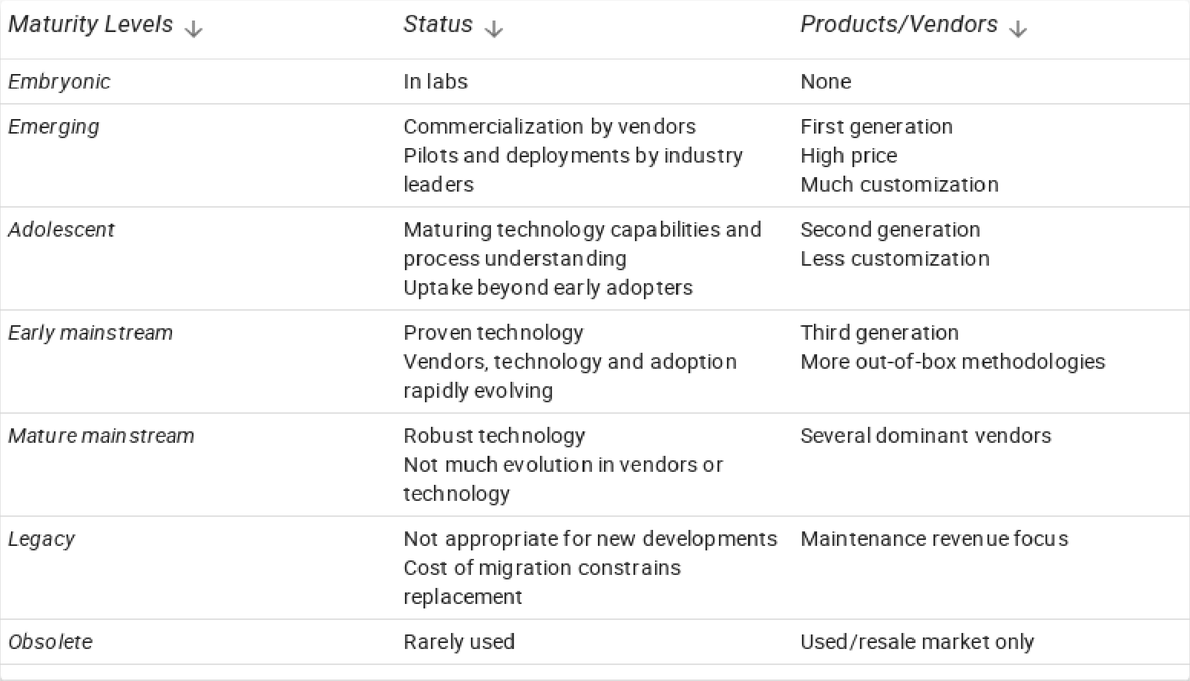
Table 3: Benefit Ratings

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)

Document Revision History

Hype Cycle for I&O Automation, 2022 - 27 July 2022

Hype Cycle for I&O Automation, 2021 - 16 July 2021

Hype Cycle for I&O Automation, 2020 - 4 August 2020

Hype Cycle for I&O Automation, 2019 - 18 July 2019

Hype Cycle for I&O Automation, 2018 - 23 July 2018

Hype Cycle for I&O Automation, 2017 - 17 July 2017

Hype Cycle for I&O Automation, 2016 - 6 July 2016

Hype Cycle for I&O Automation, 2015 - 7 July 2015

Hype Cycle for IT Operations Management, 2014 - 22 July 2014

Hype Cycle for IT Operations Management, 2013 - 23 July 2013

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

Leadership Vision for 2023: Infrastructure and Operations

Case Study: Infrastructure Platform Teams for Self-Service Delivery (Politiet)

Tool: Roadmapping Your IT Skills for the Future

Monitoring and Observability for Modern Infrastructure and Applications

Innovation Insight for Continuous Infrastructure Automation

Market Guide for Cloud Management Tooling

Market Guide for AIOps Platforms

Market Guide for Service Orchestration and Automation Platforms

Table 1: Priority Matrix for I&O Automation, 2023

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational	DevSecOps Hyperautomation	NetDevOps Observability Platform Engineering Site Reliability Engineering	Digital Platform Conductor Tools Error Budgets	

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
High	Automated Incident Response Cloud Migration Continuous Configuration Automation Vulnerability Prioritization Technology	ARO Composable Infrastructure Container Management Continuous Delivery DevOps Platforms DEX Tools GitOps Hybrid Cloud Computing Infrastructure Automation Infrastructure Orchestration Intelligent Infrastructure Network Automation Policy as Code Programmable Infrastructure SOAP Value Stream Management Platforms	AIOps Platforms Autonomous Endpoint Management Cloud Data Backup Infrastructure Platform Engineering	
Moderate	Software Asset Management Tools	Continuous Compliance Automation Immutable Infrastructure	Chaos Engineering Intelligent Automation (I&O) SMP	Intent-Based Networking
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)