Hype Cycle for I&O Automation, 2021

Published 16 July 2021 - ID G00747580 - 134 min read

By Analyst(s): Chris Saunderson

Initiatives: Infrastructure, Operations and Cloud Management

I&O automation is the catalyst that drives quality and agility as organizations adopt cloud computing and DevOps practices, and integrate AI capabilities. I&O leaders must leverage the technologies in this Hype Cycle to deliver faster value, improve efficiency and optimize costs.

Additional Perspectives

- Summary Translation: Hype Cycle for I&O Automation, 2021
  (13 October 2021)

Strategic Planning Assumptions

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, 60% of infrastructure and operations (I&O) teams will use artificial intelligence (AI)-augmented automation across enterprises, up from 1% in 2020, enabling greater IT productivity, agility and scalability.

Analysis

What You Need to Know

Automation is the foundation that enables I&O to adapt to the pace and scale of digital business, enabling speed to market and increased business agility. It profoundly affects roles, skills and expectations of I&O staff and leaders. This Hype Cycle offers insight into technologies that are pivotal to automation success.

I&O leaders responsible for automation must:

- Create a service-oriented automation strategy based on delivering a “platform as a product” (see Why DevOps Success Requires Platform Teams).
- Continue to develop software engineering skills to manage a programmable infrastructure (see How to Fix the Software Engineering Resource Gap in I&O).
- Leverage the automation architect role to drive prioritization, and enable standards and governance (see Essential Skills for Automation Architects).
- Adopt a use-case-driven approach to intelligent automation tools and AIOps platforms (see Use AIOps for a Data-Driven Approach to Improve Insights From IT Operations Monitoring Tools).
- Use automated pipelines to deliver infrastructure services (see Innovation Insight for Continuous Infrastructure Automation).

For more information about how peer infrastructure and operations (I&O) leaders view the technologies aligned with this Hype Cycle, see 2021-2023 Emerging Technology Roadmap for Large Enterprises.

The Hype Cycle

Automation is the engine that powers digital initiatives to deliver value. I&O leaders must view automation as a force multiplier for the overarching trends of programmable infrastructure, hybrid cloud computing and an engineering-driven approach to operations.

The four forces driving I&O automation technologies are:

- Adapting to support new business demands and efficiency in operating foundational platforms requires automation. The role of “developer” has expanded to include I&O, embracing programmable infrastructure and enabling emerging roles (such as reliability engineers).
- Cloud-native application deployment requires automation to drive efficient delivery and operational governance.
- Platform operations (PlatformOps) is the emerging pattern to support automated delivery and the effective support of deployed applications.
- AI techniques continue to evolve, combining AIOps and automation to extend capabilities.

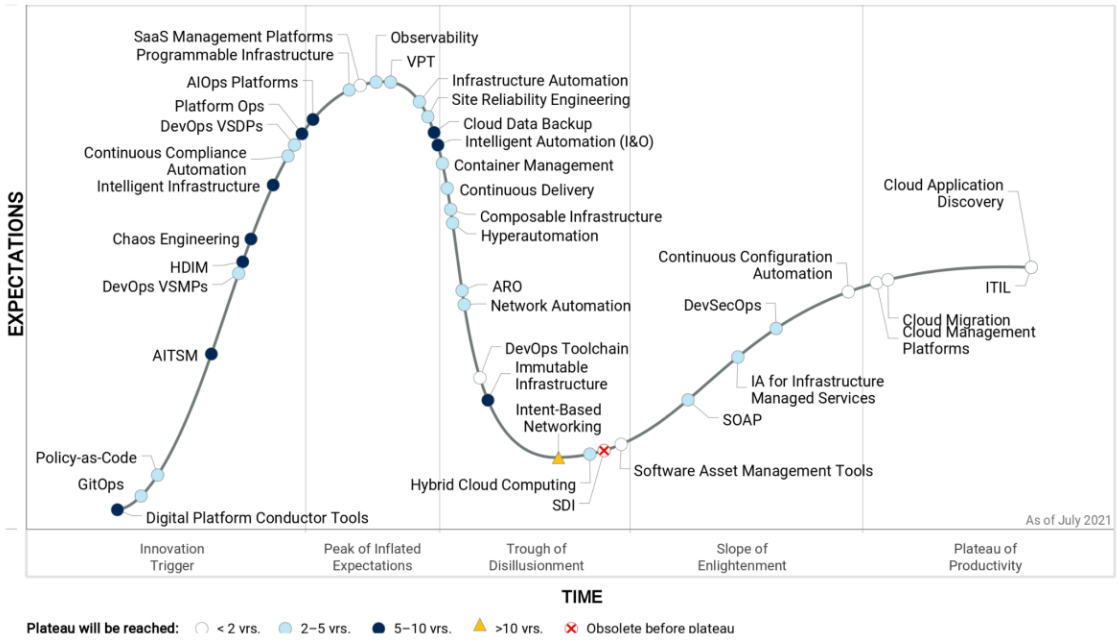
Traditional ways of implementing workload or process automation remain important efficiency and productivity investments. Technology providers have modernized these tools to include AI/machine learning (ML) techniques, and have embraced DevOps to improve the scope and quality of delivered automation. New methods of combining automation technologies to deliver hyperautomation are emerging, extending the reach and value of I&O automation into business-centric domains.

Cloud-native deployment patterns continue to impact the way that I&O manages platforms that support product delivery. Composable and programmable infrastructures take an API-driven approach to managing infrastructure in support of cloud-native delivery, highlighting the need for increased software engineering skills in I&O.

PlatformOps teams continue to transform I&O, driving an “automation first” approach. I&O leaders must embrace DevOps principles in their organizations to improve the capability and efficiency of delivery in order to make this transformation successful and valuable.

Organizations use AI to augment decision making and user experience improvement in multiple disciplines. This enables rapid feedback loops, and improves operational outcomes by speeding detection and resolution of problems. This is extending to generate improved insight related to the performance of the platforms that deliver services. For this reason, AIOps and intelligent automation technologies are rapidly gaining mind share to deliver insights and actions beyond current capabilities.

Figure 1: Hype Cycle for I&O Automation, 2021



Source: Gartner (July 2021)

Downloadable graphic: Hype Cycle for I&O Automation, 2021

The Priority Matrix

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

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

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

In the next two to five years, cloud-first and DevOps value stream delivery initiatives will drive automation investments. I&O leaders must scale the provisioning and management approaches beyond their data centers. DevOps toolchains, DevOps value stream delivery and management platforms, and disciplines such as site reliability engineering and infrastructure-centric testing that utilize the capabilities of the teams and tools that I&O makes available will become integral to support modern service delivery. Digital platform conductors will maximize the use of high-cost components, and drive intelligent workload orchestration between on-premises, edge and cloud.

Infrastructure automation enhances application delivery, supporting on-premises and cloud topologies. 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, the adoption of chaos engineering approaches will improve the resilience and availability of delivered platforms..

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

Table 1: Priority Matrix for I&O Automation, 2021

(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 Observability Site Reliability Engineering	AIOps Platforms Digital Platform Conductor Tools Platform Ops	
High	Cloud Migration Continuous Configuration Automation DevOps Toolchain ITIL	ARO Composable Infrastructure Container Management Continuous Delivery DevOps VSDPs DevOps VSMPs GitOps Hybrid Cloud Computing Hyperautomation IA for Infrastructure Managed Services Infrastructure Automation Network Automation Policy-as-Code Programmable Infrastructure SOAP VPT	Chaos Engineering HDIM Intelligent Automation (I&O) Intelligent Infrastructure	
Moderate	Cloud Application Discovery SaaS Management Platforms Software Asset Management Tools	Continuous Compliance Automation	AITSM Cloud Data Backup Immutable Infrastructure	Intent-Based Networking
Low	Cloud Management Platforms			

Source: Gartner (July 2021)

Off the Hype Cycle

DevOps has matured in its adoption and capabilities across the Gartner client base and, as such, is no longer tracked as an innovation. It remains critical for I&O to continue to implement practices and develop capabilities with DevOps both for its own purposes and in support of partner organization initiatives.

On the Rise

Digital Platform Conductor Tools

Analysis By: Roger Williams, David Cappuccio, 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 support 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 and hybrid infrastructure management tools fall short of the requirements of "anywhere operations." Moreover, as infrastructure and operations leaders struggle to manage their portfolio of investments to enable composable business, while optimizing costs and reducing risks, they need help to fill the gaps in visibility, assurance and coordination. These pressures are fueling the rise of DPC tools, which help organizations close these gaps in functionality.

Business Impact

DPC tools address the following gaps in infrastructure management toolsets:

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

Drivers

- Difficulty in maintaining an inventory of all technology infrastructure resources and their dependencies, aligned with changes to services, applications, and components and configurations of their promised performance levels.
- Lack of transparency into spending for hybrid digital infrastructure and how resource capacity aligns to 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.
- 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 will limit 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 require perfect data before they act, and vendors that design their DPC tools to only work with complete and accurate data, 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 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, risk and cost objectives, and 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

Amazon Web Services (AWS); Cloudsoft; Flexera; LeanIX; Microsoft; OpsRamp; ServiceNow; Snow Software

Gartner Recommended Reading

Innovation Insight for Digital Platform Conductor Tools

Rethink Your Infrastructure Management Tool Selection Strategy

GitOps

Analysis By: Paul Delory, Arun Chandrasekaran

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

GitOps is a technique for operating a cloud-native application using only declarative constructs stored in Git. It is the latest name for extending CI/CD to software deployment and infrastructure management. Beyond that, GitOps remains ill-defined and the subject of many debates. The CNCF's GitOps Working Group is formulating what it hopes will become the industry standard. The ideas behind GitOps are not new, but emerging tools and practices now promise to make this longtime dream a reality.

Why This Is Important

GitOps would be transformative for the I&O organization. GitOps workflows convert a Git pull request into a verified container image ready for production. Infrastructure is code. All changes flow through Git, where they are version-controlled, immutable, auditable and reversible. Developers interact only with Git, using abstract, declarative logic. I&O uses it to deploy infrastructure. It extends a common control plane across K8s clusters, which is increasingly important as clusters proliferate.

Business Impact

- **Agility and speed:** GitOps can be used to introduce version control, automation, collaboration and compliance. Artifacts are consistent and reusable. All of this translates directly to business agility and faster time to market.
- **Transparency and visibility:** GitOps artifacts are centralized and version-controlled, making them easy to verify and audit.
- **Resilience:** By implementing and centralizing infrastructure as code, GitOps enhances availability and resilience of services.

Drivers

- **Kubernetes adoption and maturity:** GitOps must be underpinned by an ecosystem of technologies, including tools for automation, infrastructure as code, CI/CD, observability and compliance. Kubernetes has emerged as a universal common substrate for cloud-native applications. This provides a ready-made foundation for GitOps. As Kubernetes adoption grows within the enterprise, so, too, can GitOps.
- **Need for increased speed and agility:** Speed and agility of software delivery is a critical metric that CIOs care about. As a result, IT organizations are pursuing tighter coupling of I&O and development teams to drive shorter development cycles, faster delivery and increased deployment frequency; 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 with process transparency and workflow commonality 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 better 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. The Working Group's draft architecture expressly requires Kubernetes and implicitly assumes the presence of a host of other technologies built on top of K8s. GitOps is necessarily limited in scope.
- **Lack of consensus:** For now, GitOps means different things to different people. This situation is likely to persist unless the GitOps Working Group succeeds in promulgating a definition that gains industrywide acceptance.
- **Cultural change:** GitOps is 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. Technology is not magic.
- **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

- **Use GitOps for cloud-native workloads:** Your initial target for GitOps must be a containerized, cloud-native application that is already using both Kubernetes and a continuous delivery platform such as Flux.
- **Embed security into GitOps workflows:** GitOps practices can and should embed security into the workflow. Security teams need to "shift left" so that the organization can build holistic CI/CD pipelines that impact software delivery and infrastructure configuration, with security embedded in every layer of that workflow.
- **Be wary of vendors trying to sell you GitOps:** GitOps isn't a product you can buy; it is a workflow and a mindset shift that needs to be part of your overall DevOps culture.
- **Use GitOps to sell automation initiatives:** I&O leaders can use the GitOps buzzword to get buy-in for adopting general automation best practices that the organization should already be doing. In the absence of a standard, you can define what GitOps means to your organization, then deploy it iteratively.

Sample Vendors

CloudBees; GitLab; Harness; Red Hat; Weaveworks

Policy-as-Code

Analysis By: Paul Delory

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Policy-as-code 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 to enforce architectural standards, corporate policies, regulatory requirements, budgets and more.

Why This Is Important

In the most mature automation pipelines, 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 end users. Now, I&O 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

- **Security, compliance and automation:** PaC combined with infrastructure automation provides direct enforcement of policies with implicit compliance guarantees.
- **Alignment of security and Ops teams:** PaC allows security and compliance teams to interface directly with automation pipelines to ensure conformance.
- **Visibility and auditability:** PaC provides both unambiguous documentation of policies and evidence they are being enforced.
- **Less toil:** PaC reduces the overhead of creating and enforcing policies.

Drivers

- **New PaC tools:** Several dedicated PaC tools are now on the market, many of them open source. Most prominent is the Open Policy Agent, a Cloud Native Computing Foundation project. But other options abound, including: InSpec (part of the Chef suite), Sentinel (part of the HashiCorp suite) and Bridgecrew (recently acquired by Palo Alto). All of the major hyperscale public clouds also have their own native policy engines.
- **Increasing regulation:** The advent of new regulations such as GDPR has 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 they are being enforced.
- **Security breaches:** Similarly, a spate of newsworthy security breaches at public companies have put every IT organization's security and compliance practices under increased scrutiny. No I&O team wants their security failures to be the reason their company ended up in the 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, which PaC can help solve.
- **Cloud optimization and cost control:** Beside their benefits for security and compliance, PaC tools can also be used to enforce the I&O department's build standards for infrastructure — including enforcing 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

- **Immaturity of tools:** PaC tools are not yet fully ripe. They 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 enables 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/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. Once PaC has proven its value, expand to other use cases over time.
- **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:** To automate a process, you must know *what* to do before you can determine *how* to do it. PaC creates specific and enforceable guidelines for automation tools to follow, solving this problem.
- **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.

Gartner Recommended Reading

Using Cloud-Native 'Policy as Code' to Secure Deployments at Scale

Innovation Insight for Continuous Compliance Automation

Market Guide for DevOps Value Stream Delivery Platforms

2021 Planning Guide for Security and Risk Management

2021 Planning Guide for IT Operations and Cloud Management

AITSM

Analysis By: Chris Matchett, Mark Cleary

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

AITSM is the optimization of IT service management (ITSM) practices to enable the application of AI, automation and analytics using the four domains (context, advice, actions and interfaces) within ITSM tools and related add-on products. The aim is to improve the overall effectiveness, efficiency and error reduction for I&O staff.

Why This Is Important

AITSM is important for intermediate and advanced I&O maturity use cases to automate and support complex environments. Its domains can extend traditional ITSM practices to provide context that aids analysis, advice that drives quick consistent decisions, and automated actions to reduce manual processes. Interfaces with AIOps tools for monitoring inputs and automation are key, and so AITSM's position is also driven by the growth of the AIOps tools market.

Business Impact

AITSM provides a framework for leveraging AI, analytics and data, leading to a reduction in incidents and an improvement in resolution times. It can automate a proportion of business consumer issues and requests, thus improving productivity as well as perception of the overall service. AITSM advice helps human agents find information faster and handle tasks more consistently. It also provides feedback by creating and updating knowledge; this can reduce costs by resolving incidents faster.

Drivers

- The “new normal” has been shaped by severe cost optimization that calls on I&O leaders to drive new efficiencies, while necessitating cuts to services using human agents.
- I&O leaders are seeking new opportunities to automate and provide more proactive management of their environments in order to both reduce costs and provide more effective service.
- Advanced ITSM tools are developing predictive and analytics capabilities, which can lead to new insights and opportunities.
- In addition to developments within ITSM tool suites, there are several vendors offering stand-alone products to work with incumbent ITSM tools.
- Initial interest in virtual support agent products and improvements in natural language processing are driving further ITSM process optimization using AI.
- Requirements for functions relating to AI, predictive analytics and automation are commonly appearing in RFPs for ITSM tools due to the benefits I&O leaders hope to leverage.
- Advances in AIOps ITOM tools are beginning to replicate ITSM tool capabilities, leading to pressure on ITSM tool vendors to improve their products.
- The number of I&O leaders evaluating features and pricing of add-on AITSM products is increasing.

Obstacles

- AI solutions and adaptive systems require data and optimized practices to learn, predict and react to, before they can deliver the promised value.
- Many organizations are too immature to take advantage of AITSM capabilities due to poorly optimized processes, weak data capture and a lack of integration with other tools and processes.
- I&O leaders expect to leverage AI add-ons for cost optimization in ITSM, yet the cost of these investments often exceeds associated benefits.
- ITSM tools currently demonstrate capability mostly in the context domain of AITSM or basic chatbots, and less commonly in advice and action domains.

User Recommendations

- Liaise with your customers to understand their perception of the support environment to prioritize the AITSM initiative in terms of cost savings, user productivity or service efficiency.
- Ensure that your ITOM and ITSM tools complement each other rather than duplicating functionality.
- Align current and desired service desk practices to the four domains of AITSM, starting with the foundational domain of AITSM context.
- Identify pockets of work that are standardized and repeatable enough to be eliminated or automated.
- Ensure that incidents are resolved with accurate diagnosis and resolution details rather than just typing “fixed.” This contextual detail is fundamental to drive AITSM advice and actions.
- Ensure compatibility between AITSM plans and the critical capabilities of currently used ITSM tools.
- Prepare to invest in skills or partners with API skills to successfully interface these tools and minisuites together to leverage best-in-class capabilities.

Sample Vendors

Aisera; BMC; Espressive; Ivanti; Moveworks; ServiceNow

Gartner Recommended Reading

Leverage 4 Domains of AITSM to Evolve ITSM Tools and Practices

Critical Capabilities for IT Service Management Tools

Market Guide to AIOps Platforms

3 Simple Ways IT Service Desks Should Handle Incidents and Requests

DevOps VSMPs

Analysis By: Hassan Ennaciri, Akis Sklavounakis

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

DevOps value stream management platforms (VSMPs) enable organizations to manage their software delivery process as a value stream to maximize the delivery of customer value. They provide visibility and traceability to every process in software delivery — from ideation through development to release and production, and extending to documenting feedback from customers. DevOps VSMPs continuously measure flow, surface constraints and non-value-added work, to improve customer value delivery.

Why This Is Important

As organizations scale their agile and DevOps practices, higher-level metrics that assess performance and efficiency of their product delivery is essential. DevOps 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 to correct course as needed. The visualization capabilities of DevOps VSMPs help product teams analyze customer value metrics against the cost required to deliver that value.

Business Impact

DevOps VSMPs help organizations bridge the gap between business and IT by enabling stakeholders to align their priorities to focus on delivering customer value. DevOps VSMPs can provide CxOs with strategic views of product delivery health and pipelines, allowing them to expedite data-driven decisions about future investments in products. 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

- Scaling agile and DevOps initiatives.
- Need for visibility into business, development and operational metrics.
- Optimization of delivery flow by mapping end-to-end processes involved in software delivery to reduce waste and bottlenecks due to cross-team dependencies.
- Need to improve quality and velocity of product deployments.
- Visibility to security and compliance status of products.
- Need for orchestration capabilities to have better traceability.

Obstacles

- DevOps VSMPs do not include native continuous integration/continuous delivery (CI/CD) capabilities; execution of the delivery pipeline requires use of a custom toolchain or a value stream delivery platform (VSDP).
- VSMPs may lack native plugins for some existing tools and that will require custom integration.
- Rationalization of acquiring another tool with more dashboards acts as an obstacle.
- VSMPs are still evolving and not all vendors have all the critical capabilities.

User Recommendations

- Ensure all stakeholders in the value streams are involved in the selection of a VSMP: business leaders, owners, application leaders and I&O leaders.
- Examine your existing EAP tools or VSDPs as some vendors are expanding their capabilities to include VSMP functionality.
- Pilot the VSMP with a product that has mature DevOps practices to best evaluate what insight can be generated.

Sample Vendors

CloudBees; Digital.ai; Opsera; Plandek; Plutora; Tasktop

Gartner Recommended Reading

The Future of DevOps Toolchains Will Involve Maximizing Flow in IT Value Streams

Agile and DevOps Primer for 2020

Flattening the Application Organization — Everyone Must Be Part of the Agile Value Stream

Predicts 2021: Value Streams Will Define the Future of DevOps

Infographic: Top 10 Technology Trends Impacting DevOps

HDIM

Analysis By: David Cappuccio, Roger Williams

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Hybrid digital infrastructure management (HDIM) maximizes application workload value across data centers, colocation and cloud providers. It involves integration of tools to manage assets and costs for devices, subnets, data centers and/or service providers. Its focus is on planning, implementing, operating and monitoring both physical and logical assets, exposing technology interdependencies and performance characteristics to enable workload optimization and operational efficiencies at scale.

Why This Is Important

Infrastructure and operations must have and provide greater insights into the performance and observability of application workloads and business services, regardless of workload location or infrastructure ownership. As cost pressures and the demand for digital business support intensify, the hype regarding HDIM is also expected to increase.

Business Impact

HDIM helps organizations visualize the existing infrastructure and any changes made over time. This improves resource utilization, which in turn leads to operating expenditure savings as resources are used more efficiently. HDIM also acts as an adjunct to IT asset management (ITAM) and problem resolution by showing how assets and resources are interrelated, not just licenses and depreciation schedules.

Drivers

- Increasingly complex infrastructures (on-premises, colocation, cloud and edge workloads and assets), requiring a detailed view of all assets and how they are interrelated.
- Enhanced problem identification, asset management, space and capacity planning and, potentially, cost optimization.
- Proto-HDIM products focused on automated discovery and dashboarding, with integrations to some domain-specific tools to provide additional data.
- Benefits like augmented workload and infrastructure visualization of complex environments that organizations are building.

Obstacles

- Individual practice experts need to see beyond their specific focus areas to support HDIM.
- HDIM vendor landscape is large, but there is little consistency in products, which puts the burden on IT to clearly understand what problem they are trying to solve.
- HDIM tools have limited integrations with existing ITAM, IT service management (ITSM), IT operations management (ITOM) and data center infrastructure management (DCIM) toolsets.
- Integration into end-to-end workflow and configuration management databases (CMDBs) is critical for mapping/tracking asset usage and movement throughout the asset's life cycle.

User Recommendations

- Begin thinking about both the tools and the skills your staff will need to support the evolving world of hybrid infrastructures.
- Map existing tools for managing technology against the functionality needed for organizing, implementing, operating and monitoring hybrid digital infrastructure to identify gaps that must be filled to maximize value.
- Work with infrastructure architects and other key stakeholders to identify options, timing and business cases for investments.

Sample Vendors

Flexera; FNT Software; Hyperview; Ivanti; Matrix42 (FireScope); OpsRamp

Gartner Recommended Reading

Innovation Insight for Digital Platform Conductor Tools

Top 10 Trends Impacting Infrastructure and Operations for 2020

Chaos Engineering

Analysis By: Jim Scheibmeir, Dennis Smith

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Chaos engineering is the use of experimental and potentially destructive failure testing or fault injection testing to uncover vulnerabilities and weaknesses within a complex system. It is systematically planned, documented, executed and analyzed as an attack plan to test components and whole systems both before and after implementation. Chaos engineering is often utilized by site reliability engineering teams to proactively prove and improve resilience during fault conditions.

Why This Is Important

Many organization's stake success on test plans that overemphasize software functionality and underemphasize the importance of validating the system's reliability. Chaos engineering (CE) moves the focus of testing a system from the "happy path" — instead, testing how the system can gracefully degrade or even continue to be useful while under various levels of impact. CE can also help identify where product documentation is less than sufficient or understanding of a system is lacking or siloed.

Business Impact

With chaos engineering, we minimize time to recovery and change failure rate, while maximizing uptime and availability. Addressing these elements helps improve customer experience, customer satisfaction, customer retention and new customer acquisition.

Drivers

- Gartner's 2020 Achieving Business Agility with Automation, Continuous Quality and DevOps Survey found that 18% of respondents were currently using or planning to use chaos engineering to improve software quality.
- Complexity in systems and increasing customer expectations are the two largest drivers of this practice and the associated tools. As systems become more rich in features, they also become more complex in their composition, and more critical to business success.
- Overall, chaos engineering helps organizations create more reliable systems and prove that systems are reliable.

Obstacles

- The first obstacle to chaos engineering is perception. Within many organizations, the predominant view is that the practice is random, done first in production, and due to these leads to more risk than less.
- Another obstacle to chaos engineering is organizational culture and attitude toward quality and testing. When quality and testing are only viewed as overhead, then there will be a focus on feature development over application reliability.
- Another common obstacle is simply gaining the time and budget to invest in learning the practice and associated technologies. Organizations must reach minimum levels of expertise where value is then returned.

User Recommendations

- Utilize a test-first approach by practicing chaos engineering in preproduction environments. Then move findings into production environments.
- Incorporate chaos engineering into your system development or testing process.
- Build-out incident response protocols and procedures, as well as monitoring, alerting, and observability capabilities in tandem with advancement of the chaos engineering 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 chaos engineering in production to facilitate learning and improvement at scale as the practice matures. However, be warned that Gartner believes that there are still very few organizations purposely using chaos engineering 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

Alibaba Cloud; Amazon Web Services; ChaosIQ; Gremlin; steadybit; Verica

Gartner Recommended Reading

Improve Software Quality by Building Digital Immunity

Innovation Insight for Chaos Engineering

How to Safely Begin Chaos Engineering to Improve Reliability

DevOps Teams Must Use Site Reliability Engineering to Maximize Customer Value

Intelligent Infrastructure

Analysis By: Philip Dawson, Nathan Hill

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Intelligent infrastructure is built from simple, repeatable infrastructure building block components from multiple sources, 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 intelligence 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 AIOps and AI/ML functions to the intelligence plane.

Business Impact

- Intelligent infrastructure builds on earlier hardware and software innovations, including CI, HCI, SDI and composable, but does not directly replace them.
- It also feeds off the application API-led programmable infrastructure that tunes infrastructure through system calls and requests.
- Intelligent infrastructure is the next innovation in delivering optimized systems for applications.

Drivers

- IT leaders now recognize cloud infrastructure, cloud platforms and cloud-native applications that drive the overall composable, programmable and intelligent infrastructure journey.
- Cloud delivery and edge expansion are fueling both infrastructure standardization and expansion to edge and IoT locations beyond remote offices/branch offices (ROBOs).
- Adding intelligence and ML 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 “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 SDI and composable, traditional system vendors often tie intelligent infrastructure to hardware-related features, which inhibits lock-in.
- Cloud management platforms are often used as overlays for cloud migrations. Intelligent infrastructure has to adapt to hybrid cloud locations, whether on-premises, provider or public cloud.

User Recommendations

- Select integrated system infrastructure solutions based on their ability to meet the current business requirements while still offering the flexibility to exploit the intelligent infrastructure innovations 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.
- Prepare for the evolution of applications and workloads by incorporating intelligence/ML infrastructure functions and persistent memory into your future system requirements.

Sample Vendors

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

Gartner Recommended Reading

Simplify Intelligent Infrastructure by Using Workload Architectures

Drive Administration, Application and Automation Capabilities of Infrastructure-Led Disruption

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, correcting and protecting against vulnerabilities resulting from coding defects and misconfiguration. It reduces manual execution steps in adhering to regulatory requirements, enhancing consistency, traceability and auditability.

Why This Is Important

Continuing DevOps initiative success drives enterprise investments in compliance automation. CCA improves release velocity and reliability while simplifying compliance enforcement via policy-driven, automated controls, improving compliance without impacting the flow of the software delivery value stream. Traditional compliance practices are incompatible with continuous software delivery processes, leading to slower delivery and unexpected, expensive remediation work.

Business Impact

Organizations evolving DevOps practices can minimize risks and penalties by embedding automated compliance 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.

Drivers

- Organizations are facing an increasing number of regulatory obligations and more stringent enforcement, so automating compliance will become even more valuable to I&O leaders as they strive to maximize flow through their DevOps value streams by: needing to scale to meet additional compliance requirements with limited delay; demonstrating compliance through automated testing; reducing the risk of compliance audit failures; and reducing the time spent in compliance steps and unexpected remediation work.
- As product teams adopt cloud-native application architectures and development models, there is a need to integrate compliance into the DevOps toolchain that supports those applications. For example, because containers are fundamentally immutable, the need to scan container images upfront requires specialized container-scanning tools for vulnerabilities. Comprehensive container security starts in development with an assessment of the contents of the container, secrets management and should extend into production with runtime container threat protection and access control.

Obstacles

- Most CCA tools only target one development or delivery activity. No vendor provides capabilities across all elements of the delivery value stream. DevOps teams must integrate multiple tools to provide compliance coverage across development and delivery activities.
- Failure to engage with compliance and security SMEs early in the development life cycle can lead to problems. Early input from compliance and security SMEs will help I&O leaders account for security and compliance requirements and audit failures.
- The lack of rule set understanding and consistent implementation can be an impediment to CCA. While it is important to leverage the acceleration that vendor rule sets can provide, it is vital that they are understood by organizational compliance teams and implemented consistently to provide 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. CCA tools enable DevOps teams to achieve both goals: improving value stream delivery and mitigating risks.
- Implement a shift-left approach to ensure compliance controls are understood 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.
- Enforce security and compliance across all domains, including databases, application code, infrastructure and open-source software. Since there is no single vendor tool that covers all those domains, DevOps teams must use multiple tools and integrate across all phases of the delivery pipeline.

Sample Vendors

Anitian; JFrog; Rapid7; Redgate; Snyk; Sonatype; Styra; WhiteSource

Gartner Recommended Reading

Innovation Insight for Continuous Compliance Automation

Market Guide for Compliance Automation Tools in DevOps

3 Steps to Ensure Compliance and Audit Success With DevOps

3 Steps to Integrate Security Into DevOps

How to Build and Evolve Your DevOps Toolchains

DevOps VSDPs

Analysis By: Manjunath Bhat

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

DevOps value stream delivery platforms (VSDPs) provide fully integrated capabilities that enable continuous delivery of software. These capabilities include planning, version control, continuous integration, test automation, release orchestration, continuous deployment (and rollback), monitoring, security testing and analyzing value stream metrics. DevOps VSDPs integrate with infrastructure and compliance automation tools to automate infrastructure deployment and policy enforcement.

Why This Is Important

Value stream delivery platforms enable organizations to simplify building and managing DevOps pipelines. They reduce complexity involved in orchestrating, integrating and governing pipeline activities. In addition, the prebuilt integration between different components of the platform leads to improved visibility, traceability and observability into the complete application development value stream. The benefits extend beyond IT.

Business Impact

VSDPs constitute the pipeline for continuous delivery of digital value. The seamless integration and shared visibility between development and operations workflows helps bridge the silos that exist between development and operations teams. Using a common platform for development, security and operations accelerates agile transformation and helps organizations adopt a product and platform team operating model. VSDPs are a foundational component of self-service platforms for development teams.

Drivers

- Continued cloud adoption and cloud-native architectures.
- Agile and DevOps ways of working with automation and collaboration being the focal points.
- Need for improved developer experience, satisfaction and productivity.
- Need for deeper collaboration and shared visibility across all IT teams (dev, sec and ops).
- Emergence of digital product and platform engineering teams to drive digital transformation initiatives.
- Competitive pressure that demands faster time to market for digital products and services.
- Proliferation of tools and the ensuing complexity of integrating those tools as well as the lack of skills to do so at scale.
- Industry traction around value stream management — VSDPs will increasingly bundle capabilities to analyze value stream metrics and extend the usability of the platforms to business stakeholders.
- Rise of vendors providing a managed open-source software (OSS)-based VSDP. Customers get the best of innovation from the OSS community and the guaranteed SLAs from a technology provider.
- Increased maturity of “as code” approaches to automate security and compliance (via policy as code) and infrastructure (via infrastructure as code).

Obstacles

- Organizations that want to unlock the full benefits of VSDPs must be willing to replace an existing toolchain — either completely or in-part. However, this is an impediment for teams that are resistant to change or view the change as a disruption to their ways of working.
- Organizations accrue technical and skills debt over time due to legacy automation workflows. That hinders teams from adopting new tools.
- The potential for vendor lock-in presents a constraint as well. Dependency on a single provider for a majority of their software development needs increases concentration risk and lowers bargaining leverage. Gartner cautions VSDP buyers that none of the vendors currently provide the full set of application delivery capabilities.
- VSDPs also fall short of providing the required value stream analytics that organizations can use to improve “flow” in the software delivery life cycle.

User Recommendations

- Scale DevOps initiatives by providing VSDPs as a self-service platform to reduce overhead, lower complexity, and ensure consistent and templatized workflows across multiple teams.
- Improve the flow of work by streamlining the software delivery life cycle with VSDPs that provide enhanced visibility, traceability, auditability and observability across the DevOps pipeline.
- Support remote development teams by adopting cloud-based VSDPs and using their integration and collaboration capabilities for code reviews, code sharing and issue tracking.
- Adopt an “as code” approach to managing IT workflows to improve operational efficiency and consistency — pipelines as code, infrastructure as code and policy as code.

Sample Vendors

Atlassian; Calculi; CloudBees; CodeNOW; Copado; Digital.ai; GitHub; GitLab; Harness; JFrog

Gartner Recommended Reading

Market Guide for DevOps Value Stream Delivery Platforms

Market Guide for DevOps Value Stream Management Platforms

The Future of DevOps Toolchains Will Involve Maximizing Flow in IT Value Streams

Why DevOps Success Requires Platform Teams

Platform Teams and AIOps Will Redefine DevOps Approaches by 2025

Platform Ops

Analysis By: Daniel Betts, George Spafford

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Platform ops is an approach to scaling DevOps that involves dedicating a team to the development and operation of a codified, highly automated, shared self-service platform. This platform team enables multiple product teams to accelerate delivery while managing quality, platform security and compliance, and standardization.

Why This Is Important

Platform ops practices are adopted by organizations needing to scale DevOps initiatives in order to reduce overlap and redundancy, enable economies of scale, and establish high standards of governance. These practices require a culture that supports learning and improvement, highly skilled automation practices, and usage of infrastructure as code (IaC) practices.

Business Impact

Using a product and platform approach can help enable the business to respond faster to threats and opportunities while also managing cost and risk. The product teams can focus on customer requirements and, in turn, the platform teams can specialize in enabling the product teams. This makes it well-suited to support digital business initiatives such as analytics, mobile applications, portals and so forth.

Drivers

- Many large organizations are adopting platform models to scale DevOps, where platform teams build standardized capabilities that enable product teams to deliver customer value.
- Difficulty in providing enough operations expertise in DevOps product teams as they scale, resulting in slower delivery cycles, software defects and frustration.
- Full-stack DevOps team structures are not scalable and often lead to duplication and competing demands that thwart long-term success.
- Challenges to ensure high standards of governance and production efficiency when product teams recreate platforms' capabilities inconsistently from team to team.

Obstacles

- Before embarking on platform ops — picking technologies, hiring a team — you should determine that platform ops is right for your organization to scale DevOps.
- If your organization is just starting DevOps or struggling to find DevOps maturity, platform ops may not be the right approach. Efforts should be focused on an iterative learning approach and scale when ready.
- Having sufficient resources to fulfill the roles required to deliver a shared platform is a challenge for many organizations.
- There can be considerable ramp-up time to enable platform team members with the software engineering, testing and programming skills needed to effectively deliver a platform.
- Organizational size and maturity to adopt platform ops can impact the decision to use platform ops.

User Recommendations

- Establish dedicated platform teams to maintain and continuously improve shared, self-service platforms. Product teams need infrastructure services that are available on-demand to deliver value faster.
- Create a cross-functional team of versatile subject matter experts to support the evolving needs of product teams. This platform team needs longevity and dedicated funding throughout the entire life cycle of the platform.
- Encourage platform team members to work closely with product teams. They must determine which tools the teams need to be more productive, provide education on how to use the platform to meet their needs and implement architectures that are conducive to shared platforms.
- Collaborate with teams other than the product teams — such as security, compliance, finance — to ensure that additional requirements are integrated into the capabilities that the platform offers. Marketing and championing the self-service platforms is critical to their success.

Gartner Recommended Reading

Why DevOps Success Requires Platform Teams

Platform Teams and AIOps Will Redefine DevOps Approaches by 2025

Using Platform Ops to Scale and Accelerate DevOps Adoption

At the Peak

AIOps Platforms

Analysis By: Gregory Murray, Pankaj Prasad

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

AI for IT operations (AIOps) platforms analyze telemetry to improve IT operations and have five characteristics: data ingestion across telemetry domains; topology assembly from network flows, application traces, hypervisor, container and cloud; event correlation to reduce the number of redundant events associated with an incident; pattern recognition to predict incidents or probable root cause; association of probable remediation to augment, accelerate or automate resolution.

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 the data to interpreting the data. AIOps capitalizes on machine learning and analytics techniques to classify and cluster diverse telemetry signals in near-real time, at scale, and in ways that exceed human capacity. Even where automated remediation is not possible, this analysis can augment and accelerate human response.

Business Impact

AIOps platforms deliver value through:

- Agility and productivity — By reducing alert fatigue through 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.
- Compounded value of existing monitoring tools — By unifying the events from siloed monitoring 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 modern, hybrid IT that relies on a complex, highly integrated mix of on-premises assets, cloud IaaS/PaaS providers and SaaS solutions to deliver their missions.
- Increasing monitoring expectations — Investments and improvements in monitoring and the pursuit of observability are generating more data from more sources. Emerging monitoring platforms and practices, 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 against other adjacent telemetry.
- Demands for reliability — Shifts in roles and responsibilities from newer 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.

As these trends, themselves, are accelerating, expect the case for AIOps platforms to continue to accelerate.

Obstacles

AIOps platform adoption must overcome the following obstacles:

- Expectations mask real opportunities — Hype is a prolific obstacle to AIOps adoption. It is hard to separate claims of intelligence and magical automation from practical, achievable use cases. Success with AIOps platforms requires clarity on the capabilities and limitations of the available solutions.
- Time to value for high-value use cases — AIOps platforms learn through observation. They learn everything from normal ranges and patterns of data to which automation resolves which issue. Learning requires time because it can take months to develop accurate detection models for rare events.

- Market shifts and maturity — AIOps is evolving and the market is in flux. Monitoring vendors are moving up the stack, AIOps platform vendors are reaching into monitoring domains, and ITSM vendors see AIOps capabilities as a way to extend their reach. Expect both technology advancements and market shifts to change what we currently understand by “state of the art” and “go to market.”

User Recommendations

- Establish clear, realistic use cases for an AIOps platform pilot. This fundamental step underpins an eventual strategy, while scoping the vendor landscape, clarifying the telemetry requirements and separating hype from reality.
- Integrate single-domain AIOps features with an AIOps platform. This approach enables efficient data ingestion and analysis, and the surfacing of insights across domains.
- Mature toward automation integration, ensuring the core benefits of AIOps are realized before full automation. High-risk cases are not ideal for automation but benefit from AIOps accelerating or augmenting human response.
- Shift mechanical operations to analytics and automated execution, while developing creative skills in integration and automation development. Prepare for disruption and adapt to a highly integrated environment. Tackle silos that can create blind spots in your AIOps platform coverage.

Sample Vendors

BigPanda; IBM; Moogsoft; ServiceNow; Splunk

Gartner Recommended Reading

Market Guide for AIOps Platforms

Infographic: Artificial Intelligence Use-Case Prism for AIOps

Solution Path for Adopting AIOps

Understanding the Application of AIOps Disciplines Within IT Operations

Programmable Infrastructure

Analysis By: Nathan Hill, Philip Dawson

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

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

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

Business Impact

Greater value (than cost reduction) can be 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. It helps reduce technical debt, and enables a sustainable and highly responsive IT infrastructure service to the business.

Drivers

- Programmable infrastructure strategies can be 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, or in the case of elastic external resources, and the termination of consumption.
- Programmable infrastructure is needed to optimize the infrastructure life cycle and more importantly enable the desired (performance, cost, speed) infrastructure provisioning in line with business demands.

Obstacles

- Cost of refreshing API-enabled infrastructure components on-premises. Applying automation to existing monolithic infrastructure components will fail due to lack of platform agility.
- Lack of maturity in APIs that enable integration across different infrastructure platforms.
- Lack of open APIs/API compatibility across vendor platforms.
- The scarcity of programmatic skills within I&O, especially in web technologies (such as HTTP and JSON) to develop these APIs.

User Recommendations

Infrastructure and operations leaders must:

- Prioritize agility as one of their top goals in pursuit of digital business outcomes.
- Implement a programmable infrastructure by investing in infrastructure automation tools and AIOps (example vendors for these markets are listed below, but no single vendor or platform can enable an organization wide programmable infrastructure strategy).
- Invest in infrastructure and DevOps, and modernize legacy IT architectures to implement an API-driven infrastructure.
- Look for reusable programmable building blocks as they extend their programmable infrastructure strategy.

Sample Vendors

Alibaba Cloud; Amazon Web Services (AWS); Google; IBM; Microsoft; Pivotal; Tencent Cloud; VMware

Gartner Recommended Reading

Programmable Infrastructure Is Foundational to Infrastructure-Led Disruption

How to Lead Digital Disruption With Programmable Infrastructure

Understand the Hype, Hope and Reality of Composable Infrastructure

How to Lead Digital Disruption With Programmable Infrastructure

Drive Administration, Application and Automation Capabilities of Infrastructure-Led Disruption

SaaS Management Platforms

Analysis By: Chris Silva, Dan Wilson

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Gartner defines SMPs as stand-alone tools that can discover, manage and secure multiple SaaS applications from a central admin dashboard, delivered as a turnkey service. The market for SMP consists of both pure-play SaaS-only management tools and SAM tools that have extended their software license and operational management to SaaS-based applications.

Why This Is Important

IT administrators lack a central dashboard to view utilization and entitlements or to centrally automate administrative tasks across the portfolio.

The market for SaaS management platforms (SMPs) has matured, with core capabilities to:

- Discover usage of SaaS applications.
- Track uptake, ongoing usage and automate workflows.
- Establish consistent identity, access and data governance controls across the SaaS estate.

Business Impact

As SMPs expand to address more SaaS applications, they will emerge as a key source of analytics data, with some vendors offering analysis of collaboration patterns among workers and across tools. This will act as a trigger to workflows in other systems and contribute to broader user experience measurement activities.

Drivers

As organizations' SaaS portfolios grow, so does the need for a single orchestration point for visibility and control. Client interest began to grow in late 2019, and Gartner has witnessed its continued modest growth in 2020. This growth is driven by:

- Continued investment in SaaS applications, which means exponential growth in admin overhead when conducted on a per-app basis. Each incoming SaaS app adds a new admin console to the mix, and with it a need to add skills unique to that application.
- Maturity of SMP tools. The portfolio of SaaS applications SMPs can manage is growing, but not every SMP will offer coverage across 100% of the SaaS estate, especially when niche or vertically-specific SaaS apps are in the mix.
- As the portfolio of managed apps grows, it is important to note that not all integrations are the same. In some cases, the SMP may be able to read information from the SaaS environment, while in other areas the SMP can both read information from, and write changes to, the SaaS environment. In almost all cases, this distinction will vary across supported SaaS apps.

Buyer awareness and product maturity have been positively impacted by recent rounds of investment into the SMP market. These range from small seed investments to eight- and 10-figure funding commitments to vendors raising capital in later-stage rounds. Despite this growth in capital, which has driven maturity and awareness of SMPs, many organizations still seek security-specific posturing tools (SSPM) to solve subsets of the SMP mandate. Others seek to gain the advantages of visibility and control over SaaS apps using CASB or WAFS functionality.

Obstacles

The growth in awareness of this class of tool is still growing. Despite an uptick in interest over the course of 2020-21 relative to established technologies, Gartner sees interest in SMPs in its early to intermediate stages of growth. Its position on the Hype Cycle and adoption reflect this.

Three forces can impact the SMP market:

- **Hybrid environments:** The reality of the app mix in many businesses requires a tool that can span management of traditional and SaaS apps, a differentiator touted by the SAM vendors making investments in SMP features.
- **Increased competition:** Infusions of investor capital have provided many (but not all) SMP vendors with resources to drive product differentiation, as well as brand and product awareness.
- **Distributed pain:** While large enterprises have begun to express interest in these tools, the distributed ownership of SaaS apps also means distributed management operations, often hiding the aggregate operational costs of the entire SaaS portfolio.

User Recommendations

Organizations looking to an SMP for better visibility of the SaaS estate must choose a tool that:

- Offers discovery capabilities that discover usage at multiple points (e.g., expense system for paid apps, identity system for apps using SSO or at the network or client level to identify traffic) in order to identify SaaS apps in use.
- Avoid acquiring incomplete solutions by reviewing the depth of integrations for each supported SaaS app. Not all SMPs will offer both read and write (bidirectional) functionality with all SaaS apps, meaning that some integrations are likely to only provide basic reporting of usage metrics.
- No SMP at this stage of the market is likely to address 100% of a large and diversified, or conversely vertically-specific SaaS application portfolio. Review whether support for key SaaS tools is present in the SMP being chosen.

Sample Vendors

AvePoint; BetterCloud; CloudM; CoreView; Intello; Productiv; Quest-Quadrotech; Torii; Zluri; Zylo

Gartner Recommended Reading

Market Guide for SaaS Management Platforms

Predicts 2021: Crisis Will Force Changes to Software and Cloud SaaS Contract Negotiation

Optimize Cost and Risk as These Software and SaaS Pricing Metrics Emerge to Enable Digital Business

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 allows them to be understood based on their outputs, and allows questions about their behavior to be answered. Tools that facilitate software observability enable observers to collect and explore high cardinality telemetry using techniques that iteratively narrow the possible explanations for errant behavior. The insights that observability provides are useful to operations, platform and DevOps teams.

Why This Is Important

The inherent complexity of modern applications and distributed systems, and the rise of practices such as DevOps, has left many organizations frustrated with legacy monitoring. These tools and techniques are unable to do more than collect and display external signals, resulting in monitoring that is only partially effective. Observability tools enable a skilled observer — often a software developer or site reliability engineer — to more effectively explain unexpected system behavior.

Business Impact

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

Drivers

The message of observability is resonating powerfully in the industry:

- The term observability is everywhere (e.g., in monitoring products, automation tools and enterprise suites) and 2021 is shaping up to be the year of observability. Although the tools are getting better, the message is being obscured by its ubiquity.
- OpenTelemetry's progress in 2021 as the "observability framework for cloud-native software" has further heightened the profile of observability and its toolchain.
- Traditional monitoring systems capture and examine (possibly adaptive) signals in relative isolation, with alerts tied to threshold or rate-of-change violations. To achieve this, one must be aware of possible issues beforehand, and instrument accordingly. Given the complexity of modern applications, it is unfeasible to do this for all potential issues.
- Observability tools enable a skilled observer — a software developer or a site reliability engineer — to more effectively explain unexpected system behavior, provided enough instrumentation is available. Integrating software observability with artificial intelligence for IT operations (AIOps) to automate subsequent determinations is a potential future development. However, such AIOps-based observability systems do not yet exist.
- Observability is an evolution of longstanding technologies and methods, and monitoring vendors are starting to include observability ideas inside their products, while new companies are building around the idea. Hence, time to Plateau of Productivity will be shorter than normal innovation profiles.

Obstacles

There are a number of obstacles to implementation of observability:

- Conservative nature of IT operations — 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 new technology is slow to be adopted.
- Many vendors, including those in the network and security domains, are using the term "observability" to differentiate their products. However, little consensus exists on the definition of observability and the benefits it provides, causing confusion among enterprises purchasing tools.
- Hyperscale cloud vendors — for example, Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) — continue to improve their observability tools. These services may reduce or eliminate the future need for third-party tools.

User Recommendations

Users starting a DevOps journey should assess software observability tools to integrate into their continuous integration/continuous delivery (CI/CD) pipelines, feedback loops and retrospectives. They should also:

- Investigate problems that can't be framed by traditional monitoring by using observability to create time and site reliability engineering (SRE) error budgeting, adding flexibility to incident investigations.
- Enable observability by selecting vendors that use open standards for collection, such as OpenTelemetry.
- Tie service-level objectives (SLOs) to desired business outcomes, using specific metrics and leverage observability tools to understand variations.
- Avoid the implication that observability is synonymous with monitoring. At a minimum, observability represents the internal, rather than external, perspective. Ideally, observability solutions make identifying unknown unknowns less onerous by identifying correlations and patterns in streams of telemetry that may escape notice.

Sample Vendors

Amazon Web Services (AWS); Chronosphere; Google; Honeycomb; Lightstep; Microsoft

Gartner Recommended Reading

Monitoring and Observability for Modern Services and Infrastructure

Magic Quadrant for Application Performance Monitoring

Cool Vendors in Monitoring, Observability and Cloud Operations

Innovation Insight for Observability

VPT

Analysis By: Mitchell Schneider

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Vulnerability prioritization technology (VPT) streamlines the vulnerability analysis and remediation/mitigation process by focusing efforts on identifying and prioritizing the vulnerabilities that pose the greatest risks to the organization. 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 approach to vulnerability management (RBVM). This class of products (and services) utilizes the telemetry from VA tools, configuration management databases (CMDBs) — although having a CMDB is not a requirement to utilize VPT — as well as application security testing (AST). VPT adds a layer of intelligence by leveraging analytics and various threat and vulnerability intelligence sources.

Business Impact

VPT solutions can be considered a form of automation that bring advanced analytics and vulnerability intelligence to reduce the human resource requirements of performing manual RBVM. The continued rise in the number of security incidents and breaches around the globe is driving many organizations to adopt VPT solutions to implement an effective, efficient vulnerability management program. The rise in incidents is also causing VA vendors to align more to the RBVM methodology.

Drivers

- The VPT market continues to grow rapidly, based on Gartner research and client inquiries, as well as sales of tools to support the process. 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 firewall [WAF]). Moreover, the solution can provide savings in terms of operational full-time employee (FTE) costs due to better prioritization, as well as reduce the organization's attack surface, preventing the vulnerabilities from being exploited.

- RBVM is an iterative process, underpinned by the technology (e.g., VA and VPT), and triggers other processes, such as IT operations executing patch management. Moreover, performing manual RBVM is challenging. It requires intelligence and automation to successfully operationalize the process. Organizations cannot handle the traditional ways of prioritizing vulnerabilities via predefined CVSS scores because they need to account for exploits and business criticality to reflect the real score to the organization. In the case of VPT, these solutions perform the analysis of vulnerabilities in the context of the current threat landscape. For example, a vulnerability that is a low risk today might be a high-impact vulnerability tomorrow due to the public availability of an exploit, while the Common Vulnerability Scoring System (CVSS) score would remain relatively static.

Obstacles

- VPT solutions are typically leveraged by organizations that are higher in terms of vulnerability management maturity and should not be used until the basic vulnerability management processes are in place. VPT will not work if there are broken processes in the VM program.
- Vulnerability management (VM) is a foundational part of information security operations. However, prioritizing vulnerabilities according to a severity score results in a response that is based on a single metric. This metric-driven output is rarely based on risk, as factors such as threat activity and asset context are not considered.
- Organizations find the exercise of VM overwhelming because of the large number of vulnerabilities showing up in the reports, which adds to the friction between other business units and the security team. The most common client inquiries that Gartner receives include: “How do I identify the top 100 vulnerabilities in my VA report?” and “How do I prioritize those vulnerabilities that matter most?”

User Recommendations

- Implement a risk-based approach that correlates asset value to calculate a risk rating leveraging VPT solutions. This reduces the risk of being breached when prioritizing remediation activities.
- 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 capabilities 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 solutions that use the context of internal security controls to maximize existing security investments. This capability is immature across the market.
- Choose VPT solutions that aggregate vulnerability data from multiple sources to present action-oriented metrics.

Sample Vendors

Brinqa; Kenna Security; NopSec; NorthStar; Risk Based Security; RiskSense; ServiceNow; Skybox Security; Tufin Software; Vulcan Cyber

Gartner Recommended Reading

The Essential Elements of Effective Vulnerability Management

How Security and Risk Management Leaders Can Establish Practical Time Frames for Vulnerability Remediation

A Guidance Framework for Developing and Implementing Vulnerability Management

Infrastructure Automation

Analysis By: Chris Saunderson

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Infrastructure automation (IA) allows DevOps and I&O teams to design and implement self-service, automated delivery services across on-premises and cloud environments. IA enables DevOps and I&O teams to manage the life cycle of services through creation, configuration, operation and retirement. These infrastructure services are then exposed via API integrations to complement broader DevOps toolchains, or consumed via a self-service catalog.

Why This Is Important

As a discipline, infrastructure automation evolved from the need to drive speed, quality and reliability with scalable approaches for deploying and managing systems. DevOps and I&O teams are using IA tools to automate delivery and configuration management of their IT infrastructure at scale and with greater reliability.

Business Impact

By enabling engineers and developers to automate the provisioning and configuration of infrastructure, organizations will realize:

- Agility improvements — continuous integration and delivery of infrastructure.
- Productivity gains — version controlled, faster, repeatable deployment.
- Cost improvements — reductions in manual effort through increased automation.
- Risk mitigation — standardized configurations across all elements driving compliance.
- Efficiency — reducing toil and enabling value-added work.

Drivers

I&O leaders must automate processes and leverage new tools to mature beyond simple deployments of standardized platforms and deliver the systemic, transparent management of platform deployments. IA tools deliver the following key capabilities to support this maturation:

- Multicloud/hybrid cloud infrastructure orchestration
- Support for immutable infrastructure
- Enable consumption of programmable infrastructure

- Self-service and on-demand environment creation
- Support DevOps initiatives (continuous integration/delivery/deployment)
- Resource provisioning
- Operational configuration management efficiencies
- Policy-based delivery and assessment/enforcement of deployments
- Enterprise-level framework to enable tooling strategy maturation

Obstacles

- Combination of tools needed to deliver IA capability can lead to an increase in tool count.
- Software engineering skills and practices are required to get maximum value from tool investments.
- Migration from point activities to infrastructure capability releases is a steep learning curve.
- IA vendor capability overlaps muddies tool landscape.
- Steep learning curves can lead to developers and administrators riveting to known scripting methods to deliver needed capabilities.

User Recommendations

- Identify existing IA tools in use to catalog capabilities and identify use cases.
- Assess existing internal IT skills to incorporate training needs to enable IA more fully.
- Baseline how managed systems and tooling will be consumed (engineer, self-service catalog, API or on-demand).
- Integrate security and compliance requirements into evaluation criteria.
- Develop an IA tooling strategy that incorporates current needs and near-term roadmap evolution (cloud adoption/proliferation).

Sample Vendors

Amazon Web Services; Chef; HashiCorp; Inedo; Microsoft; Pulumi; Puppet; Quali; VMware

Gartner Recommended Reading

Market Guide for Infrastructure Automation Tools

Innovation Insight for Continuous Infrastructure Automation

How to Build Agile Infrastructure Platforms That Enable Rapid Product Innovation

The Future of DevOps Toolchains Will Involve Maximizing Flow in IT Value Streams

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

How to Lead Digital Disruption With Programmable Infrastructure

Assessing HashiCorp Terraform for Provisioning Cloud Infrastructure

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. 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 DevOps 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 reliability of existing products or platforms as well as to create new products or platforms that warrant the investment in reliability.

Drivers

- SRE is intended to help manage the risks of rapid change, through the use of SLOs, “error budgets,” monitoring, automated rollback of changes and organizational learning.
- SRE teams are often involved in code review, looking for problems that commonly lead to operational issues (for instance, an application that does not do log cleanup and therefore may run out of storage).
- They also ensure that the application comes with appropriate monitoring and resilience mechanisms, and that the application meets SRE-approved standards or guidelines set to achieve negotiated SLOs.
- SRE practices are being adopted by organizations that need to deliver digital business products reliably. These practices require a culture that supports learning and improvement, highly skilled automation practices (and usually DevOps), and usage of infrastructure-as-code capabilities (which usually requires a cloud platform).
- SRE also uses automation to reduce manual processes, and leverages resilient system engineering principles and an agile development process that employs continuous integration/continuous deployment (CI/CD).

Obstacles

- Among the biggest roadblocks toward getting started with SRE is the conceptual foundation necessary to obtain buy-in from both management and agile or DevOps teams. SRE is a significant investment, and organizations need to organize implementation based on the mission and on the adequate budget.
- Implementing SRE without an experienced site reliability engineer requires considerable learning and improvement in order to be effective. By nature, SRE embraces risk, and this conceptual mindset is difficult for many traditional employees to completely understand.
- SRE calls for blameless analysis of understanding how teams can learn from a problem, rather than assigning blame. This means understanding what made the problem happen and how to mitigate, and publishing the results.

User Recommendations

- Engage an executive sponsor to support the initiative.
- Demonstrate sufficient value to improve credibility and support; have an acceptable level of risk.
- Build an initial SRE team with a collaborative engineering mindset and a desire to learn and improve, and automate tasks to reduce repetitive manual work.
- Define clear SLOs and service-level indicators (SLIs) to be monitored and reported against.
- Instill collaborative working between site reliability engineers and developers to help them learn how to design and build their product to meet SLOs.
- Drive an iterative approach to start and evolve SRE practices.

Sample Vendors

BigPanda; Blameless; Datadog; New Relic; OpsRamp; PagerDuty; Splunk

Cloud Data Backup

Analysis By: Jerry Rozeman, Michael Hoeck, Chandra Mukhyala

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Cloud data backup tools back up and restore production data generated in the cloud. Data can be generated by SaaS tools (e.g., Microsoft Office 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

SaaS, PaaS and IaaS providers typically offer infrastructure resiliency and availability to protect their systems from server, site or region failures but do not take responsibility for the data. When data is lost due to infrastructure failure, user or admin errors, software corruption, or malicious attacks, user organizations are fully responsible. Cloud data backup tools address these deficiencies.

Business Impact

Adopting cloud data backup tools will require significant investments in software, infrastructure, knowledge and processes, which often are not a part of the cloud business cases. However, as many of the tools can be delivered as a SaaS functionality, complexity can be significantly reduced.

Drivers

- As more production workloads migrate to the cloud (in the form of SaaS, PaaS or IaaS), it has become critical to protect data generated natively in the cloud.
- Cloud providers focus on infrastructure high availability and disaster recovery 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 Office 365 gains momentum, the need for better protection is growing rapidly, which is especially driven by Microsoft's inconsistent and incomplete use of recycle bins, requirement of retention policies, and lack of intuitive recovery processes.
- Backup of Salesforce data is the second-most-addressed workload by these vendors mainly driven by Salesforce complex and incomplete recovery of data.
- IaaS and PaaS data backup is a more nascent area that caters to organizations' need to back up production data generated in the IaaS or PaaS cloud.
- Native backup of IaaS and PaaS data usually resorts to snapshots and scripting, which may lack application consistency, restore options, data mobility, storage efficiency and policy-based automation.

Obstacles

- Deploying data protection for cloud-based workloads is an additional investment; however, this is often an afterthought, because it is not a part of the business case.
- In-depth review of each cloud vendor's SLAs is another obstacle that customers have to overcome as it limits them in their speed of cloud adoption.
- The outcome of the SLA review might block the cloud service adoption as the SLA might not meet company requirements.

User Recommendations

- Evaluate and thoroughly understand cloud-native backup and recovery capabilities, and compare them with your situations before migrating applications to SaaS, PaaS or IaaS data backup solutions.
- Ensure that contracts with cloud providers clearly specify the capabilities and costs associated with the backup solution, and understand the limitations of such solutions.
- Factor in additional backup costs into the total cost of ownership calculation before migrating to 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; Rubrik; Veeam

Gartner Recommended Reading

Magic Quadrant for Data Center Backup and Recovery Solutions

Critical Capabilities for Data Center Backup and Recovery Solutions

Market Guide for Backup as a Service

Intelligent Automation (I&O)

Analysis By: Chris Saunderson

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Intelligent automation (IA) for I&O is the application of AI techniques, advanced rule engines, heuristics and machine learning to augment decision making and automate 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 for improved business agility and reduced outage impact, and is enabling technology for hyperautomation benefits.

Why This Is Important

I&O leaders are increasingly using machine-learning-based predictive analytics and decision making to automate manual processes and go beyond scripted procedures, and also to provide insight into the delivery of value through automated toolchains. In keeping with the demand in the market, technology providers are adjusting their product focus to leverage more-advanced analytics techniques, such as decision trees, knowledge graphs, clustering, regression and classification.

Business Impact

Digital initiatives require I&O teams to be in lockstep with business requirements. IA drives data collection, updates, analyses and automation of decisions. This enables new capabilities by new automated workflows.

IA delivers benefits such as:

- Predictive capabilities (maintenance/failure effects, forecast need)
- Automated incident response (root cause, anomaly detection/execution)
- Business process management (claims processing and document matching)

Drivers

- Successful implementation of IA will leverage a high degree of cooperation between lines of business, I&O, and data and analytics teams, as well as technology providers. IA tool providers provide the underlying algorithmic implementations, connectors and data repositories, but the implementation still requires significant setup and refinement, and is never “out of the box.”
- Technology providers that offer best-of-breed tools for AIOps and RPA will influence IA. It is possible that AIOps and stand-alone RPA technology providers will expand their offerings to deliver IA, either through acquisitions or organic development. In many cases, infrastructure managed service providers white label third-party IA solutions to expand capabilities in their service offerings.
- There are three factors driving synergy between IA, AIOps and RPA:
- The buying segment (I&O leaders) overlaps across these technologies.
- The objectives are aligned — increase efficiency, scale and agility.
- The future of these innovations will increasingly be driven by AI technologies.

Obstacles

- IA, although transformative, is immature and highlights the difficulty in automation implementation.
- 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.
- There is pressure to utilize existing automation solutions to address IA use cases, even if only partially.
- IA will require a high degree of cooperation between lines of business, I&O, and data and analytics teams, as well as technology providers.
- Skills requirements 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.
- The costs of these solutions, especially related to the skills investment needed, are challenging to justify.

User Recommendations

- Define use cases by analyzing gaps in existing automation that can benefit from augmented decision making.
- 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 existing I&O procedures and documentation to help train AI models.
- Roadmap the adoption of IA as an evolution of your automation journey, keeping humans in the loop until confidence is built.
- Leverage existing investments in infrastructure managed service providers that offer IA solutions or partner with stand-alone IA tool providers.

Sample Vendors

Amelia; arago; AutomationEdge; Coretex; CSS; HCL Technologies; TCS

Sliding into the Trough

Container Management

Analysis By: Dennis Smith

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

To manage containers at scale, container management provides capabilities such as container runtimes, container orchestration and scheduling, and resource management. Container management software brokers the communication between the continuous integration/continuous deployment (CI/CD) pipeline and the infrastructure via APIs, and aids in the life cycle management of containers.

Why This Is Important

Container runtimes simplify use of container functionality and enable integration with DevOps tooling and workflows. Productivity and/or agility benefits of containers include accelerating and simplifying the application life cycle, enabling workload portability between different environments and improving resource utilization efficiency. Container management makes it easier to achieve scalability and production readiness. It also optimizes the environment to meet business SLAs.

Business Impact

Gartner surveys and client interactions show that the demand for containers continues to rise. This is due to application developers' and DevOps teams' preference for container runtimes, which have introduced container packaging formats. Developers have quickly 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

- Container runtimes, frameworks and other management software provide capabilities such as packaging, placement and deployment, and fault tolerance (for example, clusters of nodes running the application).

- The emergence of de facto standards (for example, Kubernetes) and offerings from the public cloud providers have simplified deploying containers at scale. Many vendors enable management capabilities across hybrid cloud or multicloud environments by providing an abstraction layer across on-premises and public clouds. 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.).
- Data analytics use cases have emerged over the past few years, as have operational control planes that enable the management of container nodes and clusters.
- All major public cloud service providers now offer on-premises container solutions. Independent software vendors (ISVs) are starting to package their software for container management systems.
- Some enterprises have scaled sophisticated deployments, and many more have recently commenced container deployments or are planning to. This is expected to increase as enterprises restart application modernization projects postpandemic.

Obstacles

- 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 their 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.
- More abstracted, serverless offerings may enable enterprises to forgo container management. Among these services are Knative, AWS Lambda and Fargate, Azure Functions, and Google's Cloud Run. These services embed container management in a manner that is transparent to the user.
- 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 PaaS providers' service offerings by experimenting with process and workflow changes that accommodate the incorporation of containers.
- Avoid open-source deployments unless the organization has ample in-house expertise to support.

Sample Vendors

Amazon Web Services (AWS); Google; IBM; Microsoft; Mirantis; SUSE (Rancher Labs); Red Hat; VMware

Gartner Recommended Reading

Market Guide for Container Management

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 produce valuable software in short cycles while ensuring that the software can be reliably released at any time. Through dependable, low-risk releases, CD makes it possible to continuously adapt software to incorporate user feedback, shifts in the market and changes to business strategy. This approach requires engineering discipline to facilitate the complete automation of the software delivery pipeline.

Why This Is Important

Growing DevOps initiative success continues to drive enterprise investments in CD capabilities. CD improves release velocity and reliability while simplifying compliance enforcement via automation. It is a prerequisite and a first step to continuous deployments for organizations that aspire to push changes with zero downtime.

Business Impact

CD is a key practice for a DevOps initiative that reduces build-to-production cycle time. This 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

- Agile and DevOps adoption to deliver solutions
- Need to improve release velocity and reliability
- Need to shift left and simplify compliance enforcement via automation
- Need to improve software development life cycle (SDLC) to more consistently deploy application builds and updates, buy extending the benefits of Continuous integration (CI) and automated testing to continuously build deployable software
- CD is a prerequisite and first step to continuous deployments for organizations aspiring to push changes with zero downtime

Obstacles

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

User Recommendations

- When starting a CD initiative, enterprises must consider all associated technologies and take an iterative approach to adoption. This will require collaboration with all stakeholders from product, development, security and operations.
- To enable a higher likelihood of CD success, DevOps teams must also establish consistency across application environments and implement a continuous improvement process that relies on value stream metrics.
- DevOps teams must 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.
- DevOps teams need to consider DevOps Value Stream Delivery Platforms (VSDPs) to provide fully integrated capabilities that enable continuous delivery of software.

Sample Vendors

Broadcom; Calculi; CloudBees; GitLab; Harness; JFrog

Gartner Recommended Reading

How to Build and Evolve Your DevOps Toolchains

Market Guide for DevOps Value Stream Delivery Platforms

Extend Agile With DevOps for Continuous Delivery

Composable Infrastructure

Analysis By: Philip Dawson

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Early mainstream

Definition:

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

Why This Is Important

Composable infrastructure enables resources to be aggregated through software-defined, intelligent administration and limited automation, enabling infrastructure and operations (I&O) leaders to achieve higher resource utilization and faster application deployment. Although some blade-based server infrastructures include composable networking features, composable infrastructure describes a broader spectrum of capabilities that includes disaggregation of accelerator, memory and storage resources.

Business Impact

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. Composable infrastructure helps deliver next-generation agile infrastructure, where fast development and delivery mandate rapid and continuous integration. Increased utilization of high-cost resources, such as GPU accelerators and storage-class memory, can yield financial savings.

Drivers

- Current composable implementations are limited, in that resources are pooled or restricted to using hardware from a single vendor. We saw modest steps toward greater vendor collaboration in the 2020 through 2021 time frame — for example, an agreement between next-generation, fabric consortia Compute Express Link (CXL) and Gen-Z Consortium to cooperate on standards.
- Most use cases for composable infrastructure are in multitenant environments, in which composability enables the efficient sharing of pools of accelerators or storage. Another current use case is in test and development environments, where infrastructure with varying characteristics must be repeatedly deployed.

Obstacles

- A key step in the maturity timeline for composable infrastructure will be core technology that can disaggregate DRAM from compute and balance the use of persistent memory. This is competing with DRAM and uncertain adoption.
- Composable is often tied to hardware features and functions as an alternative to software-defined infrastructure (SDI). This increases lock-in to a mixture of chassis, form factors and management tools beyond blades. It is not as portable as SDI.
- 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 infrastructure must be resized and administered frequently, or when composability increases the use of high-cost components.
- Don’t replace existing infrastructure to obtain composable infrastructure unless you have sufficiently mature automation tools and skills to implement composable features and yield benefits.
- Verify that your infrastructure management software supports composable system APIs, or that you have the resources to write your own management tools.
- Don’t avoid infrastructure with composable features. Rather, don’t choose such infrastructure, because of those features, unless you are prepared to use them and they don’t overlap with any third-party toolsets.

Sample Vendors

Cisco; Dell Technologies; DriveScale; GigaIO; Hewlett Packard Enterprise (HPE); Intel; Liqid

Gartner Recommended Reading

Understand the Hype, Hope and Reality of Composable Infrastructure

Drive Administration, Application and Automation Capabilities of Infrastructure-Led Disruption

Decision Point for Data Center Infrastructure: Converged, Hyperconverged, Composable or Dedicated?

The Road to Intelligent Infrastructure and Beyond

Hyperautomation

Analysis By: Stephanie Stoudt-Hansen, Frances Karamouzis, David Groombridge

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Emerging

Definition:

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

Why This Is Important

Leveraging multiple best-of-breed tools and processes allows providers to deliver more rapid, complex and successful automation, and allows clients to deliver orchestrated automation outcomes that distinguish them from competitors. Hyperautomation not only is about automation technologies products or services, but also is the approach of combining business process design, IT architecture deployment, governance and greater business agility to drive high competitive advantage.

Business Impact

As organizations demand greater efficiencies and outcomes from service providers, providers are leveraging hyperautomation for greater outcomes and to distinguish themselves.

- The level of efficiency that providers have achieved through automation in areas such as service desk management, hybrid infrastructures and reduction of incidents ranges from 40% to 80%.
- Gartner estimates that by 2024, organizations will lower IT and business operational costs by 30% through hyperautomation solutions.

Drivers

- Hyperautomation initiatives have grown and investment continues to increase. There was a demand prior to the pandemic and the crisis has served to accelerate the growth, as organizations seek to automate for future resilience.
- The pandemic has broken down business barriers to some employees' resistance to automation, based on the abundance of legacy, disconnected systems and suboptimal processes, creating an urgency to digitalize.
- Organizations trying to automate using a single solution, such as RPA, were failing because RPA alone can only automate tasks, not processes. They need the full suite of hyperautomation tools to achieve process automation and functional orchestration.
- Organizations are looking up to service providers for hyperautomation solutions, which draw on the orchestration of interrelated automation technologies and processes to streamline their environments and achieve greater outcomes.
- The hyperautomation approach integrates and orchestrates automation using AI, machine learning, event-driven software architecture, RPA, iPaaS, packaged software and other automation tools.
- Leveraging multiple best-of-breed tools and processes allows providers to deliver more rapid, complex and successful automation, and allows clients to deliver outcomes that distinguish them from competitors.

Obstacles

- Gartner estimates over 85% of enterprises have dozens of automation initiatives underway. These have varying degrees of success, as organizations' traditional build-up of technical debt and a patchwork of technologies have made the move to automated and hybrid environments challenging.
- Hyperautomation tools are currently immature with vendors who started from different baseline solutions (RPA, BPM and low code/no code), all descending on the same destination with a hotchpotch of tools with differing levels of maturity and integration.
- Many of the solutions are horizontal in nature being sold to a wide variety of industries, and lack the process knowledge and rules requiring investment in configuring and training the tools.
- RPA, AI and iBPMS vendors often lack the combination of technology solutions to create the best process to meet customer requirements. As a result, buyers struggle to integrate disparate complex technologies to achieve their automation goals.

User Recommendations

- Establish a mixologist approach to automation tools to avoid being overly obsessed with one technology. Avoid incorrect use by identifying vendor solutions for RPA, BPM, chatbots and optical character recognition (OCR) that can be combined to achieve the desired business outcome.
- Determine a litmus test on what needs to be automated and work with your providers to determine where you will gain your greatest ROI. Also, discuss the value of their proprietary offerings versus being vendor agnostic to avoid lock-in.
- Collaborate with your provider to create a blueprint, and continuously work to update your environments based on the hyperautomation technologies and processes that will create the greatest leverage.
- Develop automation disciplines, governance and structure within your organization by starting small with simpler automation tools such as RPA or BPM to build the foundations for wider automation.

Sample Vendors

Accenture; HCL Technologies; Hexaware; IBM; T-Systems; Wipro

Gartner Recommended Reading

Competitive Landscape: Hyperautomation Service Providers

Predicts 2021: Accelerate Results Beyond RPA to Hyperautomation

Emerging Technologies and Trends Impact Radar: Hyperautomation

Tech CEOs Must Use Hyperautomation to Enhance Offerings

Communicate the Value of Hyperautomation Using ROI

ARO

Analysis By: Daniel Betts

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Application release orchestration (ARO) tools combine deployment automation, pipeline and environment management with release orchestration capabilities to simultaneously improve the quality, velocity and governance of application releases. ARO tools enable organizations to 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 for new applications and features delivered faster to support business agility will continue growing for the foreseeable future. As a result, the resulting tumultuous and transformative activity (often in the form of DevOps initiatives) has created multiple buyers for ARO solutions. 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 their acquisition.

Business Impact

ARO tools provide transparency improvements to the release management process by making visible bottlenecks and wait states 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 the improvement. This speeds the realization of direct business value as new applications and enhancements/bug fixes can be more quickly and reliably delivered.

Drivers

By automating the deployment of code, management of environments and coordination of people in support of a continuous delivery pipeline, organizations across verticals stand to realize:

- 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 to the release process

Obstacles

- ARO remains a valuable investment for clients to make, and where vendors are able to map to client internal delivery challenges/opportunities, success will be had.
- Market has changed — the current landscape of vendors has built feature-comparable products, with some incremental differences.
- Challenge covering the space, as it is both maturing (feature parity across supplier platforms) and disrupted (the environments around the ARO space are pressing inwards on the core functionality).

User Recommendations

- Organize activities into three categories that align with ARO critical capabilities: deployment automation, pipeline and environment management, and release orchestration.
- Prioritize capabilities for current and future needs prior to evaluating vendors. The better insight you have of your current release activities, the faster you will see value from ARO.
- When evaluating ARO tools, features should be the No. 1 driver for selection. Requirements should be mapped to capabilities as part of the evaluation. 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.
- Ensure the ARO platform dashboard with release performance and underlying platforms metrics, code deployment cycles, lead time from commit to deploy, incident recovery, change failure rate and the factors that drive them.

Sample Vendors

Broadcom; CitLab; CloudBees; Digital.ai; IBM; Microsoft; Plutora

Gartner Recommended Reading

Market Guide for DevOps Value Stream Delivery Platforms

Market Guide for DevOps Value Stream Management Platforms

The Future of DevOps Toolchains Will Involve Maximizing Flow in IT Value Streams

Why DevOps Success Requires Platform Teams

Platform Teams and AIOps Will Redefine DevOps Approaches by 2025

Network Automation

Analysis By: Josh Chessman, Andrew Lerner

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Network automation tools automate the configuration, visibility, troubleshooting, reporting, and maintenance of physical and virtual network devices and services. Network automation tools can improve agility and operational efficiency, lower costs, reduce human error, and improve compliance with configuration policies.

Why This Is Important

We estimate that greater than 70% of enterprise networking activities are manual as of late 2020 (outside of public cloud environments). This lack of automation can create bottlenecks in provisioning/operations and increases likelihood of human errors, which in turn may drive outages and impact uptime. This can ultimately delay time to deliver services to lines of business (LOBs) and reduce availability of services.

Business Impact

Organizations, whether in the middle of digital transformation initiatives or not, are seeing a need for the network to become more responsive. Network automation (NA) tools allow organizations to ensure their networks meet high standards including reduced errors and support costs, improved uptime, and enhanced agility, to which users have become accustomed.

Drivers

- While organizations have been undergoing digital transformation for years, the acceleration seen in the past 12 months has drastically increased. In conjunction with this acceleration, organizations are becoming ever-more dependent on these digital initiatives to drive business value. A significant part of digital transformation is the ability for I&O to update its environment at ever-increasing rates.
- The traditional approach of manually updating each device with the appropriate settings is too slow, fraught with danger from typos and missed devices, and expensive due to increased personnel needs. Network automation tools allow organizations to make network changes across tens, hundreds, thousands, or more devices in short periods of time.
- As organizations grow, their tolerance for network outages decreases significantly. Making network changes, even with proper planning and change windows, can introduce unexpected issues that may have impacts beyond just the expected change areas. Organizations require scalable, high-quality NA tools that can effectively manage network change cycles where high change volumes and the risks of costly errors render manual changes impractical or ineffective, resulting in a need for NA tools.

Obstacles

- The skills required to implement and use these tools (such as Python or coding APIs) are often different from those traditionally associated with network engineering (such as CLI), potentially requiring additional training and staffing changes.
- Very few vendors offer NA tools that provide broad multivendor support for both Day 0/1 and Day 2 activities and strong support for WAN, campus, data center and cloud environments simultaneously. Thus, organizations struggle with tool sprawl, budget and suboptimal tools.
- While most NA tools provide support for a variety of vendor devices, there are times where vendors, products, or software or hardware revisions lack support, impacting the overall success of a deployment.
- The benefits of really good NA (versus mediocre) are apparent at the practitioner level, but can be very difficult to cost-justify the upstream investment.
- Testing and validation automation are only emerging in the NA space and are difficult to integrate with configuration change automation.

User Recommendations

- Create and maintain an accurate list of network devices with hardware and software revisions.
- Start small and iterate. Focus on nonchange/nonproduction activities first. Focus initially on tasks with less complex workflows that the network team has greater control over.
- Provide engineers appropriate time and training resources to learn the technology. Encourage them to familiarize themselves with common NA building blocks.
- Automate testing and change configuration rollback.
- Deploy NA in a practical fashion with a focus on both specific, contained areas within the organization along with nonchange activities (such as reporting and troubleshooting) before moving onto more robust functions.
- Identify tools that work with the skills within your organization and that match your organization's existing culture and workflows. For example, if your organization uses UIs for configuration changes, look for tools that do the same; if it uses CLIs for configuration changes, look for tools that operate similarly.

Sample Vendors

Cisco; Itential; Micro Focus; NetBrain; Network to Code; Red Hat

Gartner Recommended Reading

Market Guide for Network Automation and Orchestration Tools

Best Networking Practices in a DevOps WorldNetOps 2.0: Embrace Network Automation and Analytics to Win in the Era of ContinuousNext

Solution Path for Evolving to Next-Generation Enterprise Networks

DevOps Toolchain

Analysis By: Thomas Murphy

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

A DevOps toolchain comprises tools that support DevOps pipeline activities and provide fast feedback. It primarily focuses on the code to build/test/deploy sequences. While some tools support specific pipeline activities, vendors are increasingly delivering integrated solutions and supporting container-centric delivery. The center point of these solutions is the CI/CD orchestration system.

Why This Is Important

DevOps toolchains enable development and operations teams to deliver new and updated applications faster. They can include dozens of unintegrated tools, which makes automation a complex and arduous task. Our 2019 DevOps survey found that organizations have, on average, 28 toolchains, which represents a huge undertaking to create and maintain. Thus, DevOps toolchains demand greater collaboration between development and operations. DevOps cannot simply be achieved by adopting tools.

Business Impact

Delivering business value is central to DevOps. A well-designed, integrated and automated DevOps toolchain enables development and operations team members to collaborate in achieving common objectives and metrics to ensure quality, timely application delivery. DevOps teams deliver the greatest business impact when they adopt an agile mindset and have the right technology to support the activity needs of individual team members.

Drivers

- Core tooling around CI/CD is evolving, with new componentized systems that make it easier to build and maintain a build script.
- Pipelines are gaining integrated security features and evolving support around package management and containers.
- As core pipelines evolve, a new wave of broader “toolchains” is emerging around value stream delivery. We expect organizations will have multiple toolchains of the pipeline variety, and these pipelines will feed data into value stream management tools.
- The market continues to evolve via acquisitions, the emergence of open source and new commercial products, and the continued adoption of cloud architecture.

Obstacles

- Existing investments in current tools and lack of migration support dampens ROI for shift to single pipeline, and developer familiarity with existing tools slows toolchain adoption.
- Hesitancy to adopt toolchains until all capabilities are available hinders toolchain maturation. Vendors provide 80% solutions, but still require best-of-breed integrations, which leads to capability overlap or double investment.
- Shifting pricing models as vendors move from per seat to consumption meters and the shift from on-premises to cloud-based solutions, which may occur at a pace organizations aren't able to accommodate.

User Recommendations

I&O leaders and applications and software engineering leaders should:

- Develop a toolchain strategy by establishing business objectives, identifying practices to achieve those objectives and then selecting tools to support those practices. Tool selection should be the last step. When evaluating tools — even open-source options — account for the costs attached to learning, integrating and replacing them.
- Focus on removing the greatest constraint by automating development and continuous delivery processes. Each DevOps product or platform team member should understand the capabilities and contribution of each tool and work to minimize gaps and overlaps between tools. The teams should also use software engineering practices such as version control, code management and managed distribution.
- Manage and evolve DevOps toolchains securely by establishing a toolchain community of practice, using pipeline integrated security and compliance and developing effective test automation.

Sample Vendors

Amazon Web Services; Atlassian; CloudBees; Codefresh; GitLab; Harness; HashiCorp; Microsoft

Gartner Recommended Reading

The Future of DevOps Toolchains Will Involve Maximizing Flow in IT Value Streams

How to Build and Evolve Your DevOps Toolchains

Ignition Guide to Managing a DevOps Toolchain

Four Steps to Adopt Open-Source Software as Part of the DevOps Toolchain

Case Study: Manage the DevOps Toolchain as a Product (LexisNexis)

Immutable Infrastructure

Analysis By: Neil MacDonald, Tony Harvey

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Immutable infrastructure is a process pattern (not a technology) in which the system and application infrastructure, once deployed into production, is never updated in place. Instead, when changes are required, the infrastructure and applications are simply replaced from the development pipeline.

Why This Is Important

Immutable infrastructure ensures the system and application environment is accurately deployed and 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 and often applied 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, one — repair the application or image in the development pipeline and re-release into production. The result is an improved security posture with fewer vulnerabilities and 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 and will drive greater adoption.
- 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 modify or patch runtime systems.
- Although immutable infrastructure may appear simple, embracing it 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 application stacks have elements that are deployed in the form of virtual machine images. VM replacement is slower and requires greater coordination than other workload components such as containers.

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 the individual components, versioned in a source-code-control repository, then redeployed for consistency.
- Prevent unauthorized change by turning off all normal administrative access to production compute resources — for example, by not permitting SSH or RDP access.
- Adopt immutable infrastructure principles with cloud-native applications first. Cloud-native workloads are more suitable for immutable infrastructure architecture than traditional on-premises workloads.
- Treat scripts, recipes and other code used for infrastructure automation similarly to the application source code itself, which mandates good software engineering discipline.

Sample Vendors

Amazon Web Services; Ansible; Chef; Fugue; Google; HashiCorp; Microsoft; Puppet; SaltStack; Turbot

Gartner Recommended Reading

How to Make Cloud More Secure Than Your Own Data Center

Top 10 Technologies That Will Drive the Future of Infrastructure and Operations

Programmable Infrastructure Is Foundational to Infrastructure-Led Disruption

Adapting Vulnerability Management to the Modern IT World of Containers and DevOps

Intent-Based Networking

Analysis By: Andrew Lerner

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

An intent-based networking system (IBNS) is a closed-loop system to help design, provision and operate a network based on business policies. It is typically packaged as software. A full IBNS includes four key subcomponents: (1) translating higher-level business policies to network configurations; (2) automating network activities across network components; (3) having awareness of network state/health; and (4) providing continuous assurance and enabling dynamic optimization.

Why This Is Important

IBNSs simultaneously improve network agility and reliability, while enabling unified policy across multiple infrastructures.

Business Impact

A full IBNS implementation can reduce the time to deliver network infrastructure to business leaders by 50% to 90%, while simultaneously reducing the number and duration of outages by 50%.

There has been limited impact to date, due to low real-world adoption and lack of viable, easy-to-use full IBNS products. Instead, there is incremental adoption of subcomponents of IBNS, including network automation and assurance. These subcomponents are sold and implemented independent of a full IBNS.

Drivers

- The desire to make networks more agile in conjunction with cloud deployments and digital business.
- Reduced operating expenditure (opex) associated with managing networks, and more senior-level network resources free to focus on more important strategic tasks.
- Performance optimization: Intent-based algorithms provide better traffic engineering versus traditional approaches, such as routing protocols. This can improve application performance.
- Reduction in dedicated tooling costs as automation and orchestration are embedded in IBNS.
- Real-time self-documentation, which also includes the rationale (intent) behind design/configuration decisions.
- Improved compliance and simplified auditing, due to the algorithmic correctness of configurations, direct mapping to business intent, and ongoing, dynamic and real-time validation.

Obstacles

- Very few vendors provide full IBNSs. One of the reasons for this is that IBNSs are very hard for vendors to build and generalize. Instead, vendors release products that deliver some discrete benefits individually, often with limited integration between them.
- Nearly all products that are marketed by vendors as “intent based” fall short of the full capabilities of an IBNS. As of early 2021, real-world enterprise adoption of full IBNSs is nascent. We estimate fewer than 100 full deployments that meet all aspects of the definition.

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, AIOps and/or predictive analytics.
- Invest in network products that provide specific 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.

Gartner Recommended Reading

Market Guide for Network Automation and Orchestration Tools

Hybrid Cloud Computing

Analysis By: David Smith, Milind Govekar

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Hybrid cloud computing comprises one or more public and private cloud services that operate as separate entities, but ones that 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 — the cost optimization, agility, flexibility, scalability and elasticity benefits of public cloud, in conjunction with the control, compliance, security and reliability of private cloud. As a result, virtually all enterprises have a desire to augment internal IT systems with external cloud services.

Business Impact

Hybrid cloud computing enables an enterprise to scale beyond its data centers to take advantage of the public cloud's elasticity. Therefore, 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. It also sets the stage for new ways for enterprises to work with suppliers and partners (B2B) as well as customers (B2C).

Drivers

- The key driver for hybrid cloud is a desire to evolve data centers to become more cloud-like and therefore have a private cloud that has cost and other characteristics that are 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” means you have a vendor-provided private cloud offering that is packaged and connected to a public cloud in a tethered way. Azure Stack 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 hybrid cloud provides include service integration, availability/disaster recovery, cross-service security, policy-based workload placement and runtime optimization, and cloud service composition and dynamic execution (e.g., cloudbursting).
- Hybrid cloud computing is different from multicloud computing, which is the deliberate use of cloud services from multiple cloud providers for the same general class of IT service.
- Note that internally run, virtualized environments are often recast as “private clouds,” and 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.

Obstacles

- Hybrid cloud computing complements multicloud computing. Although most organizations are integrating applications and services across service boundaries, we believe that few large enterprises have implemented hybrid cloud computing beyond this basic approach — and for relatively few services. Most companies will use some form of hybrid cloud computing during the next two years, but more advanced approaches lack maturity and suffer from significant setup and operational complexity.
- Hybrid cloud is different from hybrid IT, which is 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 TCS, and other service providers and system integrators.

User Recommendations

- When using hybrid cloud computing services, establish security, management, and governance guidelines and standards to coordinate the use of these services with public and private services.
- Approach sophisticated cloudbursting 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.
- Consider cloud management platforms, which implement and enforce policies related to cloud services.
- Consider using hybrid cloud computing, if your organization implements hybrid IT, as the foundation for implementing a multicloud broker role and leveraging hybrid IT services and service providers to complement your own capabilities.

Gartner Recommended Reading

Top Strategic Technology Trends for 2021: Distributed Cloud

‘Distributed Cloud’ Fixes What ‘Hybrid Cloud’ Breaks

Predicts 2021: Building on Cloud Computing as the New Normal

SDI

Analysis By: Philip Dawson

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Obsolete

Definition:

Software-defined infrastructure (SDI) includes the broad set of software-defined infrastructure components and the software-defined data center, network, storage and compute. SDI also includes non-data-center infrastructure deployed in Internet of Things (IoT) applications and an SD edge infrastructure.

Why This Is Important

Software defined is the further abstraction of software from hardware. It enables business 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 monitoring devices or machines that are software-defined.

Business Impact

While data center SDI is embedded in other data center initiatives like cloud and hyperconverged infrastructure, SDI is now focused in key verticals operating in multiple, geographically-distributed locations (such as retail, manufacturing, retail banking, distribution and utilities). And it continues to extend IoT and non-data-center SDI initiatives for new IT operations and functions.

Drivers

- SDI data center infrastructure is well-covered with compute (SDC), network (SDN & SDWAN) 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 SDDCs, and leverages SDI benefits and features for new multimode applications and edge IoT endpoints.
- In 2021, SDIs' lingering presence of hype is enabled through the use of sensors and adapters that are abstracted through software, becoming SDI in edge, IoT and operational technology (e.g., retail POS), rather than traditional, IT-driven SDI through 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 IT operations and functions.

Obstacles

- SDI is now tied to vendor technology, not interoperability.
- SDI has now overlapped other integrated systems taxonomy like hyperconvergence, driving cloud adoption.
- In 2021, we are seeing SDI continue to release vendor-specific silo technology (not heterogeneous service driven) and, hence, is obsolete as multivendor interoperability standards and technology silos.

User Recommendations

- Extend the program to include the integration and measurement of non-data-center edge infrastructure, as SDI initiatives roll out.
- 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 storage and 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; Intel; Microsoft; Red Hat; VMware; Wipro

Gartner Recommended Reading

The Road to Intelligent Infrastructure and Beyond

Drive Administration, Application and Automation Capabilities of Infrastructure-Led Disruption

Software Asset Management Tools

Analysis By: Ryan Stefani

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Software asset management (SAM) tools help maintain compliance with licensing agreements and optimize software spending by identifying opportunities to reuse software, monitoring consumption and providing data to improve software negotiations. They facilitate this by aggregating organization's entitlement and consumption data, and then reconcile it to establish an effective license position (ELP) and properly govern the software.

Why This Is Important

SAM tools continue to draw interest within a wide variety of enterprises, regardless of industry. SAM tools are intended to help simplify the management of software assets (on-premises and SaaS) by collecting, normalizing and reconciling software consumption and entitlement data to identify optimization opportunities and noncompliance risks. Gartner has also seen SAM tools extended to support security use cases and the management of cloud consumption.

Business Impact

Managing software is a challenge for all enterprises regardless of industry, which is becoming increasingly challenging with larger software estates, complex licensing and hybrid environments. SAM tools help IT and procurement leaders simplify software management by centrally providing a consolidated view of an enterprise software estate. This ultimately improves enterprise ability to mitigate risks associated with software, optimize software spend and improve life-cycle management of software.

Drivers

- Sourcing, procurement and vendor management (SPVM) leaders often invest in SAM tools as a way to provide visibility into the software inventory to improve the enterprise's ability to manage the renewal and procurement of software.
- SAM tools also help IT finance gain insights into software expenditures for improved forecasting, cost allocation and IT financial management.
- Given the complexity of software licensing, SPVM leaders are under pressure to minimize costly, unbudgeted compliance fees associated with software vendor audits risks.
- Enterprise architects and IT security teams look to SAM tools to not only provide visibility into the entire IT estate but also enrich information such as known current vulnerabilities and exposures, end of life, and end of support, which enables enterprises to mitigate risks and plan for upgrades.
- Within infrastructure and operations, SAM tools have become a popular way to help consolidate and normalize data from various discovery and inventory sources. This cleansed data can be used to accelerate the time to value for CMDBs and service delivery.
- Organizations are continually adopting the use of cloud computing by shifting workloads to public cloud providers and introducing new SaaS applications. This is increasing the complexity of SAM by adding the need to manage the consumption of these cloud services, introducing new complex licensing rules and increasing the amount of shadow IT in organizations.

Obstacles

- Most software sourced by organizations does not comply with ISO/IEC 19770-3 standards. This standard provides a data and format structure for publishers to provide entitlement data to their customers once they've licensed software, which would enable automated loads of software entitlements. Due to the lack of adoption, loading entitlements is a resource-intensive process that is often overlooked when purchasing a SAM tool.
- While SAM tools have means to discover and inventory the IT estate, this increasing speed of change and complexity often leads to manual intervention or the use of additional data collection tools to produce an ELP.
- SAM tools administration and operation tasks, such as entitlement loading, inventory sources health checks and remediation actions based on the ELPs, require a specialty set of skills, which many organizations underestimate. This often leads to failed SAM tool implementations and initiatives.

User Recommendations

- Establish a clear and realistic scope by determining which three to five publishers are initially in scope and building upon that to add additional publishers.
- Determine what license metrics, environments (e.g., IaaS, SaaS), operating systems and virtualization technologies are involved with your inscope publishers. This will help evaluate and select the appropriate SAM tool(s) for your enterprise.
- Use the out-of-the-box integrations with existing inventory sources, where available, and regularly monitor data for accuracy. If data quality is poor or lacking, add or evaluate additional data sources to address gaps.
- Evaluate SAM managed service providers to complement investments in a SAM tool and address their limitations as well as augment resources for tool administrations and operations such as entitlement loading.

Gartner Recommended Reading

Magic Quadrant for Software Asset Management Tools

Critical Capabilities for Software Asset Management Tools

Software Industry Transformation Requires Software Asset Management Programs to Follow Suit

Climbing the Slope

SOAP

Analysis By: Chris Saunderson

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Service orchestration and automation platforms (SOAP) enable foundational workload automation and support for event-driven business models and cloud infrastructure. I&O leaders must use platforms for service orchestration and automation to drive customer-focused agility as a part of cloud, big data and DevOps initiatives.

Why This Is Important

The foundational capabilities of workload automation platforms are being leveraged to respond to increased business agility demands. SOAP enable efficient management of scheduled tasks as well as extend to event- and integration-driven architectures. Delivery across new topologies and against new demands requires evaluating and modernizing practices and tooling related to business processes delivered.

Business Impact

Digital ecosystems expanding beyond the on-premises data center require rethinking of the ways in which business processes are executed. Further, continued cost and skilled staff pressures are leading to evaluation of current capabilities and investment into cost-optimized or supportable capabilities. Organizations seeking to modernize their workload automation capabilities should therefore add SOAP to their technology roadmap.

Drivers

- New and evolving business climates that require greater speed of change implementation of change and less tolerance for delay.
- Agile delivery techniques, requiring evolution of platform capabilities.
- Self-service access to create business automation workflows.

- Limitations in existing tooling, surfaced by hybrid execution topologies that span on-premises, hybrid and cloud platforms.
- SaaS-first requirements.
- SOAP supplier cost and licensing changes, forcing evaluation of the market and alternative suppliers.
- Business risk posed by fragility and complexity of existing processes.

Obstacles

- Foundational capabilities are difficult to displace, as efficiencies rely on process execution.
- Reliability is expected of existing solutions, and disruption due to migration between suppliers is perceived as risking that reliability.
- Adoption of SaaS platforms is seen as risky, both from a compliance and availability perspective.
- Skilled resources to sustain existing platforms and implement new ones are difficult to find.

User Recommendations

- Ensure that a full catalog of business processes (including criticality assessment) being executed through traditional workload automation or workflow automation platforms is maintained.
- Align SOAP services to new or evolving business demands by identifying adoption of cloud-native services or event-driven architectures for roadmap purposes.
- Assess organizational interest in SaaS-delivered offerings to shape supplier evaluation criteria.
- Utilize licensing changes as a catalyst to evaluate suppliers in the SOAP market.

Sample Vendors

Ayehu; BMC; Broadcom; HCL Software; PagerDuty (Rundeck); Redwood; Resolve; ServiceNow; Stonebranch; Tidal Software

Gartner Recommended Reading

Market Guide for Service Orchestration and Automation Platforms

How to Start Executing a Successful Automation Strategy

Move Beyond RPA to Deliver Hyperautomation

IA for Infrastructure Managed Services

Analysis By: Stephanie Stoudt-Hansen, David Groombridge

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Gartner uses the overarching term “intelligent automation” to cover a variety of technologies. These range from rapid-automation technologies (i.e., robotic process automation software or scripting) to AI approaches, such as deep learning, machine learning, cognitive techniques, NLP, speech recognition and machine vision. Intelligent automation (IA) for infrastructure managed services is the application of these technologies to IT infrastructure operations, delivered through managed services.

Why This Is Important

Where service delivery relies on manual processes, IA can be used for routine parts of work to decrease human effort, provide cost efficiencies and reduce potential errors. Leading service desk providers can use IA to resolve 40% to 80% of contacts and can automate 80% to 95% of the provisioning and management of hybrid infrastructure services. This automation is now extending further into related services such as application administration, smart buildings and security services.

Business Impact

IA in infrastructure managed services offers a number of potential benefits:

- Gartner expects contracts containing IA to show annual cost savings of 2% to 8% for commodity services, depending on the specific service and the extent of its use.

- Furthermore, IA makes it easier for enterprises to scale rapidly to demands rather than hiring new people, requiring annual pay raises, PTO or additional hiring due to staff turnover.

Drivers

- Infrastructure service providers continue to enhance their automation capabilities by embedding intelligent automation deeper in their platforms and existing infrastructure services.
- Artificial intelligence also generates analytical insights that allow for proactive and preventative maintenance actions to help reduce system downtime and impact to users.
- IA provides rapid scaling, multilanguage, reduced business impact, repeatable quality, and the ability to refocus staff on more value-added business needs. All of this drives improved user satisfaction and SLA delivery.
- Organizations buying infrastructure managed services have come to expect their service providers to offer year-over-year savings, with step-down pricing during multiyear contracts.
- In the past, providers delivered this through industrialization of services and use of low-cost labor in a global delivery model.
- Increasingly, buyers should expect that savings will now be achieved by “automation arbitrage,” in which IA replaces a substantial part of the human labor in provider offerings.

Obstacles

While IA is increasingly available, obstacles to leveraging it in managed service contracts can still be challenging:

- Penetration of these services into enterprises is increasingly common but not yet universal, with existing contracts often seeing little change until renewal, because it was not part of the original contract.

- Most infrastructure services providers have their own automation tools, which provide integration and orchestration of third-party automation tools. This has allowed providers to expand their capabilities from simple task automation into process automation and orchestration. Although this can be good for clients, it also can create lock-in if solutions are customized.
- Some providers are also beginning to sell their automation tools as stand-alone solutions, and offer outcome-based "automation-as-a-service" offerings, which are only paid for on the basis of cost reductions achieved. Understanding the pricing and whether providers can achieve these offerings will require careful due diligence from SPVM.

User Recommendations

The critical component needed to make IA work is a substantial and detailed data record. For infrastructure managed services, AI systems learn by tracking the actions of engineers during incident resolution and by identifying patterns in logs of incident, change or other data, and how each was addressed. Organizations preparing for increased use of AI now and in the future should:

- Ensure that all log data and any related metadata is contractually available in the future, even if an external service provider currently maintains it. Furthermore, the contract must require such data to be comprehensive, clear and complete through defined quality criteria.
- Ensure, where possible, that technologies leveraged by managed service providers are vendor agnostic and can be abstracted to avoid vendor lock-in.
- Incorporate step-down forward pricing in contracts, coupled with regularly-increasing targets for SLAs, predicated on the use of additional automation.
- Track the percentage of automated processes in any managed service monthly to avoid the provider trying to deliver annual cost reductions by cutting staffing levels without automating.

Sample Vendors

Atos; Cognizant; Hexaware; IBM; TCS; Wipro

Gartner Recommended Reading

Market Guide for Intelligent Automation Leveraged for IT Managed Services

Scale Infrastructure Operations With Intelligent Automation and a Central Knowledge Unit

Contract for Best-in-Class Performance for Data Center and Cloud Managed Services

DevSecOps

Analysis By: Neil MacDonald, Mark Horvath

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Early 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 protection at runtime as well.

Why This Is Important

As IT development processes become more agile (including shifts to DevOps operating models), security should be proactively and seamlessly integrated into them — DevSecOps. DevSecOps offers a means of effectively integrating security into the development process, eliminating or reducing friction between security and development, and pragmatically achieving a secure, workable software development life cycle (SDLC).

Business Impact

The goal is to enable development to move faster without compromising on security and compliance. Furthermore, the externalization of security policy enables business units and security organizations, not developers, to define appropriate policies. 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 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 developer's existing workflows, not require them to learn skills seemingly unrelated to their goals.
- The use of open source has greatly increased the risk to the inadvertent use of known vulnerable components and frameworks by developers.

Obstacles

- Developers view security testing tools as slowing them down in getting new releases out.
- Implemented incorrectly, siloed and cumbersome security testing is the antithesis of DevOps.
- Developers don't want to leave their development (continuous integration/continuous delivery [CI/CD]) pipeline to view 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, frustrating developers.
- The diversity of developer tools used in a modern CI/CD pipeline will complicate seamless integration of DevSecOps offerings.

User Recommendations

- Prepare security and risk management teams for automated integration with DevOps initiatives, and identify the primary skills and technology gaps.
- “Shift left” and make security testing tools and processes available earlier in the development process, ideally as the developers are writing code.
- As zero vulnerability applications aren’t possible, favor automated tools with fast turnaround times with a focus on reducing false positives and allowing developers to concentrate on the most critical vulnerabilities first.
- Prioritize the identification of open-source software (OSS) components and vulnerabilities in development (referred to as software composition analysis).
- Require your security vendors to support out-of-the-box integration with common development toolchain vendors and also support full API enablement of their offerings for automation.
- Require security controls to understand and apply security policies in container- and Kubernetes-based environments.
- Favor offerings that can link scanning in development (including containers) to correct configuration and protection at runtime.

Sample Vendors

Apiiro; Aqua Security; Contrast Security; IBM (Red Hat), NowSecure; Palo Alto Networks; ShiftLeft; Snyk; Sonatype; Veracode

Gartner Recommended Reading

12 Things to Get Right for Successful DevSecOps

Integrating Security Into the DevSecOps Toolchain

Market Guide for Cloud Workload Protection Platforms

Magic Quadrant for Application Security Testing

Critical Capabilities for Application Security Testing

Market Guide for Software Composition Analysis

How to Make Cloud More Secure Than Your Own Data Center

DevSecOps Security Metrics: Use Your Code Repository to Start a Virtuous Cycle

Continuous Configuration Automation

Analysis By: Chris Saunderson

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Continuous configuration automation (CCA) tools enable infrastructure administrators and developers to automate the deployment and configuration of systems and software. They support the description of configuration states and settings, and the deployment of software binaries and configuration data. Most CCA tools have open-source heritage, and some offer commercial support. Commercial CCA tools have vendor support, role-based administration and advanced management capabilities.

Why This Is Important

CCA tools have proven critical to operational efficiency and enabling DevOps initiatives by their ability to manage and deliver infrastructure and associated software and configuration changes as code. CCA tools have continued to expand their reach into networking, containers, patching, compliance and security use cases, enabling programmatic assessment and the remediation of configuration deltas. They also offer a framework for the automation of Day No. 2 operations of delivered systems.

Business Impact

By enabling automation of the deployment and configuration of settings and software programmatically, organizations realize:

- **Agility improvements** — continuous integration/delivery for infrastructure and operations (I&O) infrastructure management
- **Productivity gains** — repeatable, version-controlled infrastructure deployment
- **Cost optimization** — reductions in manual interventions by skilled staff

- **Risk mitigation** — automated compliance using standardized, documented processes and configurations

Drivers

- Organizations need a broader set of deployment and automation functions beyond configuration management, including: infrastructure-as-code (IaC); patching; application release orchestration (ARO); configuration auditing (e.g., for regulatory or internal policy compliance); and orchestration of operational tasks.
- Enabling an automation framework that enables deployment automation and Day No. 2 operational automation of changes, compliance and response to incidents or problems
- Imperative for infrastructure administrators to mature from task-based scripting to a more-structured approach to automation and delivery
- Need for repeatable, standardized deployments available to an end-user or I&O administrator that enables quick delivery of infrastructure to meet end-user needs and I&O policies and baselines.

Obstacles

- Confusion in the capabilities in automation tools leads to assumptions and misunderstandings of capabilities.
- Developers and administrators may use CCA on an insular basis, further inhibiting enterprisewide adoption.
- IT skill sets hinder adoption of these tools, requiring source code management and software engineering skills to make full use of capabilities.
- The growing use of immutable infrastructure has created confusion about the role of CCA tools; however, CCA tools and containers can be used in a highly complementary manner.

User Recommendations

- Clarify the role 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.
- Costs associated with CCA tools extend beyond just the licensing cost: Both professional services for enablement and training requirements should be included in cost evaluations.
- Expect to invest in training because not all infrastructure administrators have the skills needed to use these tools successfully.
- Guard against developers and administrators reverting to known scripting methods to complete specific tasks in place of using CCA capabilities.
- DevOps and IT operations leaders maximize the value of CCA tool investments by ensuring that their organizations' culture can embrace CCA tools strategically.

Sample Vendors

CFEngine; Chef; Inedo; Puppet; Red Hat; SaltStack

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

Entering the Plateau

Cloud Management Platforms

Analysis By: Dennis Smith

Benefit Rating: Low

Market Penetration: 5% to 20% of target audience

Maturity: Mature mainstream

Definition:

Cloud management platforms (CMPs) enable organizations to manage private, public and multicloud services and resources. Their functionality combines provisioning and orchestration; service request management; inventory and classification; monitoring and analytics; cost management and resource optimization; cloud migration, backup and disaster recovery; and identity, security and compliance. Functionality can be provided by a single product or a set of offerings with some degree of integration.

Why This Is Important

Managing a workload after it has migrated to the cloud is as important as the initial cloud migration. Enterprises will deploy CMPs (often as a part of a larger product suite) to increase agility, reduce the cost of providing services and increase the likelihood of meeting service levels. Costs are reduced, and service levels are met, because CMP deployments require adherence to standards, as well as increased governance and accountability.

Business Impact

- CMPs provide the functionality to address initial provisioning of cloud resources, as well as ongoing management.
- The recent CMP market focus has been on preventing enterprises from overspending or leaving themselves vulnerable to security issues — two key items to avoid when adopting cloud services.

Drivers

- Organizations need to address multicloud requirements. In some cases, they want to manage public services that were often acquired by lines of business (LOBs) outside the infrastructure and operations (I&O) organization and have become difficult to manage.
- Vendors are addressing the key issues enterprises face. Many vendors are looking to combine cost management and security functionality into governance tooling. A few vendors are also looking to provide infrastructure as code (IaC) assistance by overlaying cloud management functionality to this capability.
- In addition, many vendors have added container management to their CMP offerings. The ability to serve both application developers and I&O personas is key. This requires CMPs to be linked into the application development process to enable I&O teams to enforce provisioning standards, without imposing a workflow that inhibits agility.
- Desirable IT outcomes include: policy enforcement; reduced lock-in to public cloud providers, although at the cost of CMP vendor lock-in, which can slow innovation; enhanced ability to broker services from various cloud providers and make informed business decisions as to the providers to use; ongoing optimization of SLAs and costs; management of SLAs and enforcement of compliance requirements; health and performance monitoring of cloud applications; accelerated development, enabling setup/teardown of infrastructure that mimics production, resulting in lower overall infrastructure costs and higher quality (this can be in support of DevOps initiatives); and movement of complex workloads into the cloud that require best-in-class capabilities from multiple public cloud providers resulting in a multicloud adoption model.

Obstacles

- **Market evolution.** The CMP market continues to change, with vendors and enterprise customers getting a better feel for where such tooling can and cannot be used.
- **Evolving customer requirements.** Challenges vendors face include interfacing with multiple public clouds, cost transparency with workload optimization to remediate cost overruns, handling newer functions (e.g., containers and serverless deployments), and edge computing.

- **Market consolidation.** Many CMP vendors are acquiring cost management vendors and incorporating their functionality into their products. Vendors in adjacent markets are acquiring CMP vendors and combining this functionality with asset management and SaaS operational management. Cloud service providers (CSPs) and management service providers (MSPs) are entering the market, and many long-standing vendors have introduced next-generation products that target gaps in their previous products.

User Recommendations

- Weigh your full vertical (infrastructure as a service [IaaS], platform as a service [PaaS] and SaaS) and horizontal (on-premises, public cloud and edge) needs.
- Choose between native cloud services and CMPs by identifying a preferred provider model. Favor native cloud services if you value depth with a cloud provider; choose CMPs you want breadth across cloud providers.
- Determine the utility of functionally focused tools by defining the organization's functionality needs. Integrate cloud management or traditional management tools, because no vendor has a total cloud management solution.
- Ensure staffing to operate CMP platforms by planning new roles (e.g., cloud architects).
- Develop skills in financial and capacity management.
- Enable aggregation, integration, customization and governance for multicloud adoption models and environments by establishing a unified consumption layer via the Multicloud Management Platform (MCMP) or the Material Cost Management System (MCMS).

Sample Vendors

CloudBolt; Flexera; Morpheus Data; Scalr; Snow Software; VMware

Gartner Recommended Reading

Market Guide for Cloud Management Tooling

Market Guide for Container Management

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 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.
- A recent and well-justified emphasis on application modernization as part of migration has further confused 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 MSP, 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.
- Ensure you 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; Bespin Global; Capgemini; Cognizant; Deloitte; Logicworks; Rackspace Technology; Smartronix; Tata Consultancy Services; Wipro

Gartner Recommended Reading

Magic Quadrant for Public Cloud Infrastructure Professional and Managed Services, Worldwide

Critical Capabilities for Public Cloud Infrastructure Professional and Managed Services, Worldwide

Cloud Cost Scenario Planning Tool

Ignition Guide to Creating a Migration Plan for Public Cloud

Cloud Application Discovery

Analysis By: Jay Heiser

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Cloud application discovery (CAD) is a mechanism that provides information on which public cloud services are being accessed. Discovery reports include application name and type, and usage by individual and department. Information on cloud services in use is vital for a variety of corporate functions, including security, licensing, compliance and I&O.

Why This Is Important

Most organizations have hundreds, even thousands, of SaaS applications in regular use, many of which the IT department is unaware of, and most of which are not IT's direct responsibility. Cloud application discovery mechanisms identify and report on this "unsanctioned IT," a critical first step for any organization which wants all public cloud use to be secure, compliant with regulation and usage agreements.

Business Impact

Organizations that have chosen to explicitly manage use of SaaS and cloud services with CAD-type mechanisms are often able to noticeably reduce SaaS expenditures. Organizations that govern the use of SaaS experience significantly less frustration with service renewal and are less likely to experience downtime or security incidents.

Drivers

- IT professionals increasingly recognize that identification and analysis of unsanctioned services are critical elements of data governance, cybersecurity and IT spend management. This recognition drives uptake of CAD. Regulations, especially the EU GDPR and CCPA, provide additional incentive to determine which SaaS platforms are in use to determine whether that use is consistent with regulatory requirements.
- CAD is not a stand-alone market, but rather a feature of several categories of multifunction management tools. It is a primary capability of cloud access security broker tools and SaaS management platforms, and a secondary capability of software asset management, DNS solutions, firewalls and secure web gateway products.
- Although the level of actual CAD utilization remains surprisingly low, the widespread inclusion of this feature in a variety of product categories means that most organizations can apply it if they wish.

Obstacles

- Surprisingly, CAD is available to most organizations through existing tools, although no offerings include the full set of capabilities needed by every corporate function with a stake in understanding and managing the external applications being used. Dozens of multifunction products offer different forms of CAD functionality, typically as an add-on feature to some other more strategic security, license management or SaaS management function.
- The CAD reporting of these tools is usually aimed at one of those corporate constituencies, and may not be in a form that supports the cloud control needs of other organizational departments. Most organizations have a relatively low concern about shadow IT.
- Without a top-down mandate to control the use of SaaS, security and procurement leaders rightly recognize that the rest of their organization would prefer that they not report on the significant use of SaaS. Consequently, CAD features are often underutilized, or not used at all.

User Recommendations

- Start by reviewing expenditures in corporate accounting records to see which cloud services are being purchased off the IT budget.
- Extend visibility across free services and services paid for by individuals by using CAD tools that draw from the activity logs of firewalls. Secure web gateways provide a relatively convenient source of data on all external sites that are accessed from the corporate network.
- Route all remote traffic to the enterprise through a VPN (which is relatively uncommon) if your organization is highly motivated to track the cloud access activities of travelling and work from home systems. Ensure that all remote systems are routing all traffic through a Secure Web Gateway, or install a CAD mechanism that uses a local agent.
- Use CAD mechanisms with risk priority reporting to help IT security, privacy, compliance and other IT governance functions focus their attention where it can be most impactful.

Sample Vendors

Bitglass; Censornet; Eracent; Flexera; McAfee; Microsoft; Netskope; Scalable Software; Snow Software; Broadcom (Symantec)

Gartner Recommended Reading

Market Guide for SaaS Management Platforms

Magic Quadrant for Cloud Access Security Brokers

How to Develop a SaaS Governance Framework

ITIL

Analysis By: Mark Cleary

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

ITIL is an IT service management (ITSM) framework owned by AXELOS, a joint venture between the U.K. government and Capita. It describes practices that define, design, deploy and manage products and services delivered by IT. ITSM activities are collated as practices to address specific aspects of service support and delivery (e.g., managing incidents or changes), negotiating service levels, or managing assets or capacity. The latest evolution, ITIL 4, was published in February 2019.

Why This Is Important

ITIL satisfies the business demand for available, stable and resilient IT services with a framework of service-focused practices. The framework is all encompassing, recognizing that effective delivery requires as much focus on the strategy and design as it does on support. A successful implementation will deliver standard, repeatable and consistent processes that can reduce costs, improve business productivity and deliver the expected business outcomes.

Business Impact

- Better support to the delivery of business outcomes, improving the business' confidence in IT
- Improved business productivity and reduced costs through standard and repeatable practices
- Standardized and codified IT plans and managed delivery of its services
- A recognizable interface with the business for the day-to-day management of IT services
- Improved competence and capabilities of the IT organization
- Assistance to transform IT from a technology focus to a service focus

Drivers

- The need to improve the overall delivery of IT services
- The need to meet business outcomes with an investment in a set of standard and repeatable practices focused on the planning, management, delivery and support of IT services
- The need to remove the inconsistent approaches, lack of accountability and planning, and the variance in service quality inherent in technology-focused organizations
- The need for an effective interface with the business for interactions relating to the provision of IT services
- Effective ITIL implementations, which are a key dependency in improving the maturity of IT
- The need for effective planning and management of risk to maintain service availability
- The removal of IT silos by adopting and implementing standard ways of managing and supporting IT services

Obstacles

- ITIL implementations fail because the culture is technology-focused, and ITIL practices are seen as unnecessary, bureaucratic and slow by the IT staff.
- A lack of focus on the change in working practices results in staff resistance, especially when they realize that their roles and responsibilities are changing.
- Many implementations create an inward-looking organization that focuses on the process, rather than the need to meet business objectives.
- Many IT organizations lack governance and fail to measure the performance of their services, resulting in a loss of business value and poor adherence to the practices.
- Too many IT organizations buy an ITSM tool designed for greater maturity. This results in pressure to implement more ITIL practices, even though the organization's competence and capability is insufficient to justify the investment.
- Senior IT managers often align with staff when challenged about practices that inhibit them, undermining the investment and value of ITSM.

User Recommendations

- Determine the business expectations of the IT organization in managing services.
- Design and implement an effective organizational change management program to continually engage and address staff concerns regarding ITSM.
- Ensure that senior IT managers understand and support the need for ITIL practices.
- Focus on designing and deploying effective incident and change management practices first.
- Implement and measure key performance indicators (KPIs) for each practice, and review and improve them with effective governance and continual service improvement.
- Do not buy an ITSM tool designed for a more-mature organization.
- Improve the maturity of ITSM with a focus in other areas, including accountability, business relationships, people competencies and capabilities, service-focused roles and stakeholder support.
- Align with DevOps and product teams to understand their requirements and address them with lean, agile practices adaptable to the different needs of the IT organization.

Gartner Recommended Reading

Modernize ITSM to Meet the Demands of DevOps and Product Teams

What I&O Leaders Need to Know About the ITIL 4 Foundation

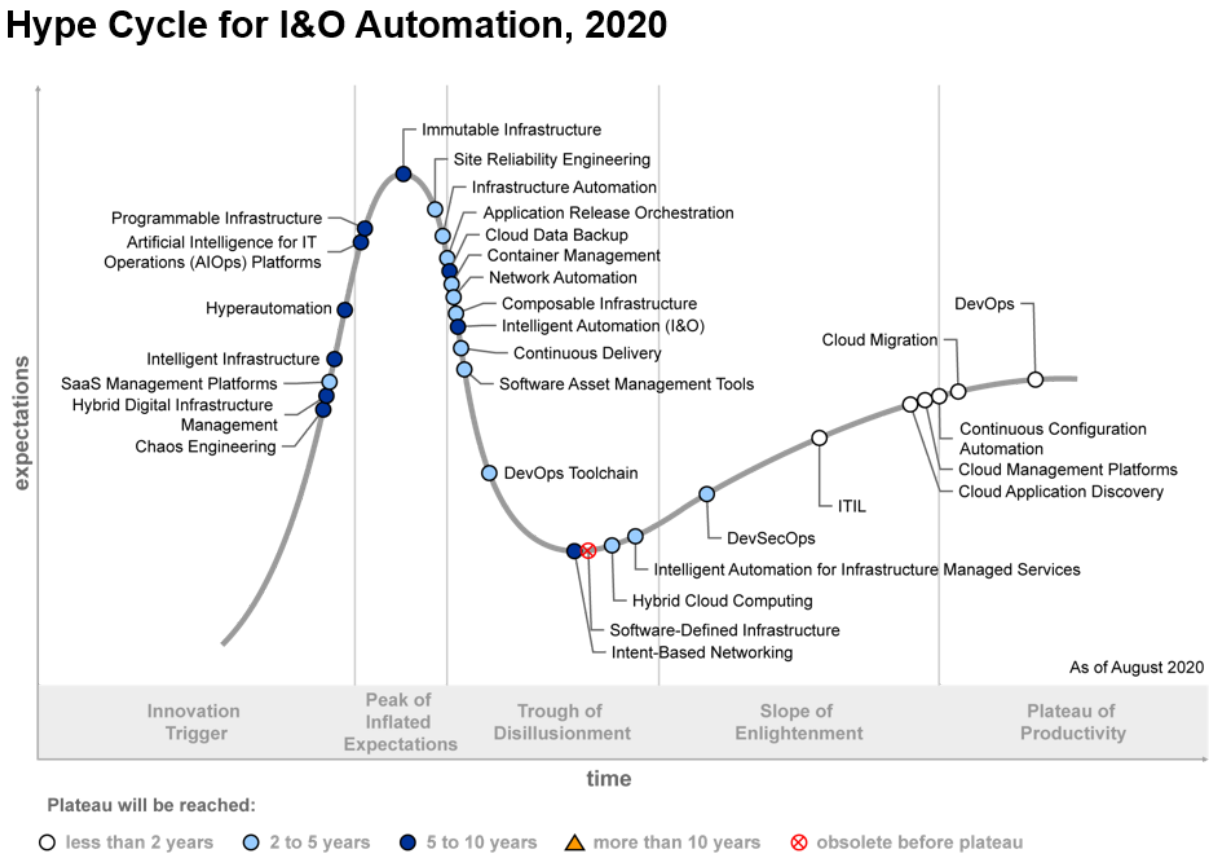
Three Steps to Agile ITSM

How to Organize IT for Efficiency

How to Structure IT like a Service Provider

Appendixes

Figure 2: Hype Cycle for I&O Automation, 2020



Source: Gartner
ID: 441834

Gartner

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 2021)

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 2021)

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 2021)

Document Revision History

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 Author

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

Understanding Gartner's Hype Cycles

Leadership Vision for 2021: Infrastructure and Operations

Quick Answer: How Should I&O Leaders Introduce Software Engineering Skills to DevOps Platform Teams?

Innovation Insight for Continuous Infrastructure Automation

Innovation Insight for Chaos Engineering

Market Guide for Cloud Management Tooling

Market Guide for Service Orchestration and Automation Platforms

Predicts 2021: Accelerate Results Beyond RPA to Hyperautomation

How to Build and Evolve Your DevOps Toolchains

Predicts 2021: Value Streams Will Define the Future of DevOps

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

Table 1: Priority Matrix for I&O Automation, 2021

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational		DevSecOps Observability Site Reliability Engineering	AIOps Platforms Digital Platform Conductor Tools Platform Ops	

Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
High	Cloud Migration Continuous Configuration Automation DevOps Toolchain ITIL	ARO Composable Infrastructure Container Management Continuous Delivery DevOps VSDPs DevOps VSMPs GitOps Hybrid Cloud Computing Hyperautomation IA for Infrastructure Managed Services Infrastructure Automation Network Automation Policy-as-Code Programmable Infrastructure SOAP VPT	Chaos Engineering HDIM Intelligent Automation (I&O) Intelligent Infrastructure	
Moderate	Cloud Application Discovery SaaS Management Platforms Software Asset Management Tools	Continuous Compliance Automation	AITSM Cloud Data Backup Immutable Infrastructure	Intent-Based Networking

Benefit ↓	*Years to Mainstream Adoption*			
	Less Than 2 Years ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Low	Cloud Management Platforms			

Source: Gartner (July 2021)

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 2021)

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 2021)

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 2021)