# Hype Cycle for I&O Automation, 2020

**Published:** 4 August 2020 **ID:** G00441834

**Analyst(s):** Chris Saunderson

Automation is a catalyst that drives consistent quality and business 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.

## Table of Contents

Analysis....3
- What You Need to Know....3
- The Hype Cycle....3
- The Priority Matrix....5
- Off the Hype Cycle....7
- On the Rise....7
  - Chaos Engineering....7
  - Hybrid Digital Infrastructure Management....8
  - SaaS Management Platforms....10
  - Intelligent Infrastructure....12
  - Hyperautomation....13
- At the Peak....15
  - Artificial Intelligence for IT Operations (AIOps) Platforms....15
  - Programmable Infrastructure....17
  - Immutable Infrastructure....19
  - Site Reliability Engineering....21
  - Infrastructure Automation....23
  - Application Release Orchestration....25
  - Cloud Data Backup....27
  - Container Management....29
  - Network Automation....30
- Sliding Into the Trough....32

Composable Infrastructure....32
Intelligent Automation (I&O)....33
Continuous Delivery....35
Software Asset Management Tools....37
DevOps Toolchain....39
Intent-Based Networking....40
Software-Defined Infrastructure....43
Hybrid Cloud Computing....44
Intelligent Automation for Infrastructure Managed Services....45
Climbing the Slope....47
DevSecOps....47
ITIL....49
Cloud Application Discovery....51
Cloud Management Platforms....52
Continuous Configuration Automation....54
Entering the Plateau....56
Cloud Migration....56
DevOps....58
Appendixes....60
Hype Cycle Phases, Benefit Ratings and Maturity Levels....61
Gartner Recommended Reading....62

## List of Tables

Table 1. Hype Cycle Phases....61
Table 2. Benefit Ratings....61
Table 3. Maturity Levels....62

## List of Figures

Figure 1. Hype Cycle for I&O Automation, 2020....5
Figure 2. Priority Matrix for I&O Automation, 2020....6
Figure 3. Hype Cycle for I&O Automation, 2019....60

# Analysis

## What You Need to Know

Automation is the foundation that enables organizations to cope with the pace and scale of digital business, enabling speed to market and business agility. It profoundly affects roles, skills and expectations of infrastructure and operations (I&O) 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 "How to Manage and Market Platforms as Products for DevOps Teams").
- Invest in software engineering skills to manage a programmable infrastructure (see "How to Fix the Software Engineering Resource Gap in I&O")
- Appoint an automation architect 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").

For more information about how peer I&O leaders view the technologies aligned with this Hype Cycle, see "2020-2022 Emerging Technology Roadmap for Large Enterprises."

## The Hype Cycle

Automation is the thread that weaves digital initiatives together to deliver value. I&O leaders must view automation against 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:

- Digital business mandates automation. This creates a demand for software engineering skills within I&O to support programmable infrastructure and emerging roles (such as reliability engineers).
- Adoption of cloud requires automation of application deployment, operational governance and infrastructure delivery.
- DevOps is becoming mainstream, driving platform operations as the approach for automated delivery of infrastructure services.
- Artificial intelligence (AI) techniques "automate the automation," combining AIOps and automation to extend capabilities.

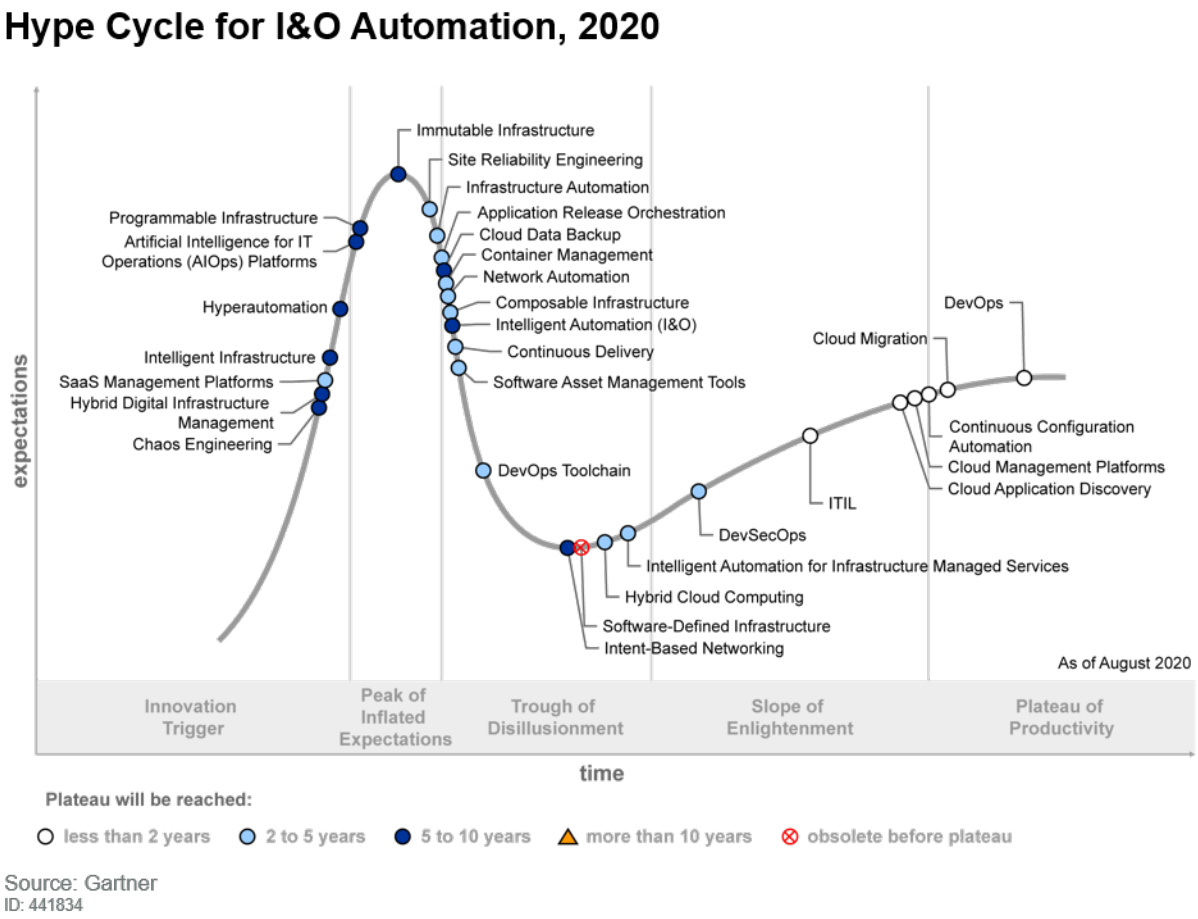
Cloud adoption continues to impact the way that I&O manages platforms. Composable and programmable infrastructures take an API-driven approach to managing infrastructure, highlighting the need for increased software engineering skills in I&O.

DevOps momentum continues to ripple across 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. Fundamentally, I&O must transform itself as technology transforms; adopting DevOps practices will make this transformation successful and valuable.

Organizations use AI to augment decision making and user experience improvement. This enables rapid customer feedback loops, and improved operational outcomes by speeding detection and resolution of problems. For this reason, AIOps and intelligent automation technologies are rapidly gaining mind share to deliver insights and actions beyond current capabilities.

None of this implies that traditional ways of implementing workload or process automation are less important. Technology providers have modernized these tools to include AI 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.

Figure 1. Hype Cycle for I&O Automation, 2020




Source: Gartner
ID: 441834

## 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 adoption and DevOps initiatives will drive automation investments. I&O leaders must leverage cloud management platforms, container management and cloud migration technologies to scale beyond their data centers. Composable and intelligent infrastructure will maximize the use of high-cost components, and drive intelligent workload location between on-premises, edge and cloud.

Infrastructure automation enhances the cadence of application delivery. Programmable and immutable infrastructure technologies present a robust architectural pattern where organizations

replace rather than update in place, leveraging cloud principles. Although these software-defined technologies require new skills, the presence of these skills is a good indicator of the maturity of automation in an organization.

Increased use of AI techniques as part of AIOps and intelligent automation will enable I&O teams to improve the speed and accuracy of decisions and actions. Future IT operations automation will be more intelligent and will need intelligent automation tools to deliver higher-value business services using intelligent automation tools. Infrastructure service providers are responding to this need as they enhance their automation capabilities with AI and embed intelligent automation in their existing infrastructure services.

Figure 2. Priority Matrix for I&O Automation, 2020

## Priority Matrix for I&O Automation, 2020

| benefit | years to mainstream adoption | | | |
|---|---|---|---|---|
| | less than two years | two to five years | five to 10 years | more than 10 years |
| transformational | **DevOps** | **DevSecOps**<br>**Site Reliability Engineering** | **Artificial Intelligence for IT Operations (AIOps) Platforms** | |
| high | **Continuous Configuration Automation**<br>**ITIL** | **Application Release Orchestration**<br>**Composable Infrastructure**<br>**Container Management**<br>**Continuous Delivery**<br>**DevOps Toolchain**<br>**Hybrid Cloud Computing**<br>**Infrastructure Automation**<br>**Intelligent Automation for Infrastructure Managed Services**<br>**Network Automation**<br>**Software Asset Management Tools** | Chaos Engineering<br>Hybrid Digital Infrastructure Management<br>Hyperautomation<br>Intelligent Automation (I&O)<br>Intelligent Infrastructure<br>Programmable Infrastructure | |
| moderate | **Cloud Application Discovery**<br>**Cloud Migration** | SaaS Management Platforms | Cloud Data Backup<br>Immutable Infrastructure<br>Intent-Based Networking | |
| low | Cloud Management Platforms | | | |

**As of August 2020**

Source: Gartner
ID: 441834

## Off the Hype Cycle

Intelligent automation subsumes the technology capabilities provided by IT process automation, IT service orchestration and heuristic automation. This trend reflects the current buying patterns and direction pursued by process automation technology providers. I&O leaders are increasingly looking to use machine-learning-based predictive analytics and decision making to augment human decision making, and mature that decision making to drive automation of manual processes beyond scripted procedures.

Machine-learning-augmented data centers (ML-augmented DCs) as a stand-alone segment has been integrated into the intelligent infrastructure market. This is a natural evolution forward for this market, where technology providers have transitioned to providing more integrated solutions that holistically address data center technology and management markets.

## On the Rise

### Chaos Engineering

***Analysis By:*** Jim Scheibmeir; Dennis Smith

***Definition:*** Chaos engineering is the use of experimental and potentially destructive failure 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 pre- and postimplementation. CE is often utilized by site reliability engineering teams to proactively prove resilience during fault conditions, and to eliminate those potential sources of system downtime.

***Position and Adoption Speed Justification:*** Chaos engineering has emerged from the practices first pioneered by Netflix (such as Chaos Monkey, Chaos Kong and the Simian Army) and Google (via their DiRT exercises). Early efforts at chaos engineering took simple actions (such as unexpectedly killing a virtual machine). The practice is moving beyond innovative early adopters and being utilized in leading enterprises in the financial services and online retail industry. While there continues to be substantial interest in the wider IT community, chaos engineering will eventually find its way to more enterprises over the next few years as many mature their digital initiatives.

As companies attempt to build scalable, highly available systems, they must demonstrate resilience in the face of not only worst-case scenarios (such as unexpected load and component outages), but also “corner case” and cascade events that start from minor issues. The practice is moving beyond innovative early adopters and becoming integrated into leading enterprises in the financial services and online retail industry. There continues to be substantial interest in the wider IT community, and it will find its way to more enterprises over the next few years as many commence their digital initiatives.

***User Advice:*** We recommend the following:

- Utilize a test-first approach by practicing chaos engineering in preproduction environments and move findings into production environments.
- Incorporate as a part of your system development and/or testing process.
- Build-out incident response protocols and procedures, as well as monitoring, alerting, and observability capabilities in part with advancement of any 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.
- As your practices mature, investigate opportunities to use chaos engineering in production to facilitate learning and improvement at scale, although we believe that there are still very few organizations purposely using it in their production environments.
- While not a security technique, chaos engineering does sometimes discover security issues.
- By adopting and then extending chaos engineering with autoremediation and continuous validation in the live operational environment, a "digital immune system" may be developed within an application or system.

***Business Impact:*** With chaos engineering, we minimize time to recovery and change failure rate, in addition to uptime and availability — all of which help improve customer experience, customer satisfaction, customer retention and new customer acquisition.

***Benefit Rating:*** High

***Market Penetration:*** 1% to 5% of target audience

***Maturity:*** Adolescent

***Sample Vendors:*** Alibaba Cloud; Bloomberg; ChaosIQ; Gremlin; Microsoft; Netflix; OpenEBS; Verica; VMware

***Recommended Reading:*** "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"

"Not Just Microservices: Choose the Right Service Granularity for Your Applications"

"Market Guide for Service Orchestration and Automation Platforms"

"Maverick* Research: Software Testing and the Illusion of Exterminating Bugs"

## Hybrid Digital Infrastructure Management

***Analysis By:*** David Cappuccio; Roger Williams

***Definition:*** HDIM is a toolset for maximizing application workload value across owned data centers, colocation and cloud service providers. It involves the integration of tools designed to manage technology assets and costs for devices, subnets, domains, data centers and/or service providers. Its focus is on planning, implementing, operating and monitoring both physical and logical assets. This provides a clear picture of the technology interdependencies and performance characteristics to enable workload optimization and operational efficiencies at scale.

***Position and Adoption Speed Justification:*** Over the next five years, we expect an HDIM toolset will emerge that is a superset of DCIM today. This is in response to a growing realization that I&O must have and provide greater insights into the performance 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 expected to intensify.

Some proto-HDIM products are focused on automated discovery and dashboarding, with integrations to some domain-specific tools to provide additional data. While domain-focused solutions will continue to be needed for detailed activities within a given technology stack, there is a lack of support for solutions that can provide an overall view of performance and coordinate actions that can improve the overall balance of technology value, cost and risk. These HDIM tools will provide a coordination point for the broader toolset of HDIM that organizations will need to take full advantage of hybrid digital infrastructure.

***User Advice:*** The HDIM market is in the very early stages of development. I&O leaders and data center managers need to begin thinking about both the tools and the skills their staff will need to support this evolving hybrid world. These are not replacement tools, but rather they augment workload and infrastructure visualization of the complex environments that organizations are building:

- Bring together subject matter experts from I&O teams to discuss hybrid digital infrastructure management challenges on a regular basis. Supplement these conversations with insights from sourcing and procurement, IT, finance, applications, and enterprise architecture team members as appropriate.
- Strengthen infrastructure architecture capabilities to account for the increased complexity of workload support. This may include specific roles for cloud, edge, automation and other technology domain work.
- 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 their value. Work with infrastructure architects and other key stakeholders to identify options, timing and business cases for investments as appropriate.

***Business Impact:*** HDIM tools help organizations visualize and optimize their infrastructure changes (both major and minor) that are made over time. The resulting improvements in resource utilization can lead to operating expenditure savings as resources are used more efficiently. More importantly, this kind of optimization can enable IT managers to defer capital or operating expenditure by ensuring that allocated resources are used as efficiently as possible. HDIM also acts as an

important adjunct to IT asset management by showing how major assets and resources are interrelated, not just licenses and depreciation schedules.

***Benefit Rating:*** High

***Market Penetration:*** 1% to 5% of target audience

***Maturity:*** Emerging

***Sample Vendors:*** CloudSphere; Device42; Flexera; FNT Software; Hyperview; Ivanti; LogicMonitor; Matrix42-FireScope; OpsRamp; Turbonomic

***Recommended Reading:*** "Predicts 2020: IT Operations"

"Hybrid Digital Infrastructure Management: A View From the Top"

"Market Trends: The Future Operations of Infrastructure MSPs Will Require an Equilibrium of Enterprise IT and Digital Business"

## SaaS Management Platforms

***Analysis By:*** Chris Silva

***Definition:*** SaaS management platforms (SMPs) provide three core functions in the management of SaaS applications: discovery of known and unknown SaaS apps in use, workflow automation of management tasks across disparate SaaS tools and the unification or augmentation of platform-specific security functions. The key benefit of SaaS management platforms is the ability to use a single tool to manage a varied set of SaaS tools in use.

***Position and Adoption Speed Justification:*** All enterprise-class SaaS applications offer their own, native management functions, but IT administrators lack a central dashboard to view utilization and entitlements or centrally automate IT administrative workflows across multiple SaaS applications. These tools are a key ingredient to manage SaaS applications at scale and consistently apply policies for use and data security.

The continued uptake of SaaS applications, such as productivity suites (G Suite, Office 365), storage (Box, Dropbox) and function-specific tools (Salesforce, Workday) have contributed to growing management overhead for IT operations leaders. Initially this market was populated by tools focused on one, specific type of application, but Gartner has witness the market evolve in the past year with multiple vendors branching out and broadening the number of SaaS applications these tools can address. Gartner believes the ability to address multiple SaaS applications as an increasingly important asset for competing in this market.

Buyers and vendors face a similar challenge, finding the right mix of tools supported (for buyers) and the right mix of tools to support (for vendors.) Once top-tier broadly used SaaS applications are supported, there is a large opportunity cost for adding additional, but more niche SaaS applications; for buyers, taking on a tool that only addresses a portion of the SaaS environment undercuts the value of adopting an SMP. As such, Gartner expects vendors to continue growing their portfolio of

SaaS applications, but at a slowing pace. Buyers will see grater disparity among vendors in their support for “long tail” SaaS applications that are specific to their region, vertical market or support a diverse best-of-breed SaaS environment.

SMPs represent one of several SaaS security and control planes. Some of the capabilities overlap with tools such as cloud access security brokers and software asset management but are complementary to, not replacements for these technologies. The hallmark of these tools is the focus on SaaS applications and while they may expand to take on on-premises applications as well, Gartner sees this as a potential future development in this market, not a core element of the SMP.

Gartner has accelerated the speed at which we expect SMP to reach its next phase on the Hype Cycle for 2020. This is due to the 2020 COVID-19 pandemic’s impact on remote working which has driven more investment in SaaS tools. This investment is creating a proliferation of tool-specific management tasks for the growing SaaS portfolio while also increasing scrutiny of costs and utilization of IT assets; two areas SMPs can directly address.

***User Advice:*** In organizations looking to bring on an SMP to help increase the visibility of the SaaS application estate, it is critical to choose a tool with discovery capabilities. Using browser plug-ins, network access information and by ingesting financial data these tools will outline which tools are being used, both those sanctioned by IT and those adopted by users without IT’s involvement. Many vendors will define “discovery” to mean better usage visibility of tools IT has formally adopted, but lack the ability to detect SaaS apps unknown to IT, providing incomplete visibility, management and risk profiling.

Ensure that the support for key SaaS tools is present in the SMP being chosen, paying particular attention to the depth of functionality for each, supported SaaS application. Due to the varying availability and complexity of the APIs used by the SMP, it is not uncommon to see disparity of SMP function between supported SaaS applications.

Understand that vendors are in varying stages of maturity in their support for functionality in securing data and apps, discovering user-adopted SaaS and breadth of application support, making direct comparisons between many SMPs difficult.

***Business Impact:*** SMPs provide many of the efficiency, risk mitigation and total cost of ownership (TCO) benefits of IT operations management tools, extended to the SaaS application estate. SaaS applications often lack sufficient IT management capabilities forcing organizations to choose between delaying adoption or accepting suboptimal management capabilities. SMPs extend management and security capabilities to bridge these gaps and minimize trade-offs between manageability and need for a given SaaS application.

Large IT organizations often rely on scripting (for example, through PowerShell) to automate bulk tasks, produce custom reports and fill gaps in the native SaaS administrative console. This can be time-consuming and detract from consistency in control (due to lack of clear ownership, regular updating and revision or peer review). SMPs can reduce or eliminate the amount of scripting administrators must use to manage their SaaS environments.

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

***Benefit Rating:*** Moderate

***Market Penetration:*** 5% to 20% of target audience

***Maturity:*** Adolescent

***Sample Vendors:*** AvePoint; BetterCloud; CoreView; Intello; Pointr; Productiv; Quadrotech; ShareGate; Torii; Zylo

***Recommended Reading:*** "Market Guide for SaaS Management Platforms"

"How to Cut Software and SaaS Costs and Quickly Improve Cash Flow in Times of Crisis"

"How to Evaluate SaaS Providers and Solutions by Developing RFP Criteria"

## Intelligent Infrastructure

***Analysis By:*** Philip Dawson; Nathan Hill

***Definition:*** Intelligent infrastructure is built from simple repeatable 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 and tuning as software overlays.

***Position and Adoption Speed Justification:*** Intelligent infrastructure encapsulates intelligence and machine learning (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. Adding intelligence and ML on top of this infrastructure composition capability ensures that infrastructure is always optimized for the application load. Intelligent infrastructure additionally adds or feeds the AIOps and AI/ML functions to the intelligence plane. The intelligence plane automates infrastructure and workload provisioning to application consumption.

***User Advice:*** I&O leaders contemplating intelligent infrastructure should accommodate three considerations:

- Select integrated systems 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.

***Business Impact:*** Intelligent infrastructure builds upon 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. In intelligent infrastructure, the "control plane" is enhanced with automation driven by infrastructure analytics ML, to become an "intelligence plane."

***Benefit Rating:*** High

***Market Penetration:*** 5% to 20% of target audience

***Maturity:*** Emerging

***Sample Vendors:*** Cisco Systems; CU Coding; DDN; Hewlett Packard Enterprise (HPE); IBM; Intel; Microsoft; VMware

***Recommended Reading:*** "Simplify Intelligent Infrastructure by Using Workload Architectures"

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

## Hyperautomation

***Analysis By:*** Stephanie Stoudt-Hansen; Frances Karamouzis; David Groombridge

***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 decision, and process and/or task automation tools). Hyperautomation-related services refer to the strategy, design, implementation and managed services offered by service providers to leverage one or more hyperautomation technologies.

***Position and Adoption Speed Justification:*** Gartner estimates that over 70% of commercial enterprises have dozens of automation initiatives underway. However, these have met with varying degrees of success, as organizations' traditional build-up of debt and a patchwork of technologies have made the move to automated and hybrid environments challenging. Instead, organizations are now looking 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. This 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. The reality of automation technologies are they are not a future concept. Organizations and service providers have been leveraging them for decades to gain efficiencies through a number of different initiatives and often in a disparate and siloed fashion. Hyperautomation is not about automation technologies products or services alone, it's the approach

of combining business process design, IT architecture deployment, governance and greater business agility to drive competitive advantage at a higher order of magnitude.

***User Advice:*** As organizations continue to demand greater efficiencies and business outcomes from managed service providers, the providers are leveraging hyperautomation to achieve greater outcomes and distinguish themselves among their competitors. The level of efficiency that service providers have achieved through automation in areas such as service desk provision, management of hybrid infrastructures and reduction of incidents ranges from 30% to 80%. The efficiency achieved depends on the ability of the service provider to automate and the area of infrastructure. This was the first wave of leveraging individual automation technologies to drive efficiencies. The next wave is through the combination of automation and intelligent tools in a continuous process driven by strategy, architecture and planning to achieve further efficiencies — hyperautomation.

Organizations preparing for increased use of hyperautomation now and in the future should:

- Drive hyperautomation decisions by identifying where a hyperautomation approach is required instead of a traditional automation approach by working with IT and business stakeholders to identify processes that change frequently, are heavily integrated across systems but which are highly repetitive in nature. Incorporate these requirements into your service provider agreements through contractually linked business outcomes. Look for continuous improvement and document the metrics supporting the end results.
- Determine a “litmus” test on what needs to be automated and work with your providers to determine where you will gain your greatest return on investment (ROI). Providers have the capabilities to help you benchmark and flag both short-term and long-term impact on your investments and drive greater impact. Also, discuss the value of their proprietary offerings versus vendor agnostic to avoid lock-in.
- Collaborate with your provider to create a blueprint or roadmap, and continuously work to update your environments based on the hyperautomation technologies and processes available or that will create the greatest leverage.

***Business Impact:*** Competitive pressures for efficiencies and returns are forcing organizations to seek the best in breed and strategic relationships with their service providers. Gartner estimates that by 2024, organizations will lower IT and business operational costs by 30% by combining hyperautomation technologies with redesigned operational processes. The concept of hyperautomation is constantly in automation flux and does not neatly fit into one process or tool. Infrastructure service providers will therefore need to continually work with organizations on a business-driven approach. They need to rapidly identify, determine and automate in a defined and disciplined fashion. The providers that embrace these concepts and processes will gain competitive advantage and drive greater results for their customers and be seen as a strategic partner. Hyperautomation is the continuous build on the intelligent automation journey.

***Benefit Rating:*** High

***Market Penetration:*** 1% to 5% of target audience

***Maturity:*** Emerging

***Sample Vendors:*** Capgemini; Cognizant; HCL Technologies; IBM; Infosys; NTT DATA; T-Systems; TCS; Wipro

***Recommended Reading:*** "Top 10 Strategic Technology Trends for 2020: Hyperautomation"

"Move Beyond RPA to Deliver Hyperautomation"

"Tech CEOs Must Use Hyperautomation to Enhance Offerings"

"Communicate the Value of Hyperautomation Using ROI"

"Predicts 2020: Sourcing and Procurement Application Technology Disruptions"

## At the Peak

### Artificial Intelligence for IT Operations (AIOps) Platforms

***Analysis By:*** Charley Rich; Pankaj Prasad

***Definition:*** Artificial intelligence for IT operations (AIOps) platforms combine big data and machine learning through support of all primary IT operations functions through the scalable ingestion and analysis of the ever-increasing volume, variety and velocity of data generated by IT operations. The platform enables the concurrent use of multiple data sources, data collection methods, and analytical and presentation technologies.

***Position and Adoption Speed Justification:*** Increased demand for AIOps platform capabilities is fueled by the growing need to intelligently drive the acceleration and automation of IT operations functions through analysis of both historical and real-time data. This is happening as roles and responsibilities converge (with DevOps and SRE as a leading examples) in the pursuit of greater agility as well as the ever increasing momentum behind digital transformation. The desire to intelligently drive automation requires continuous insights derived from machine learning algorithms based on data generated by ITOM disciplines like APM, ITIM, NPMD, DEM and ITSM. AIOps platform adoption — in particular, machine-generated data including logs, metrics and traces, as well as human-processed data such as incidents dependencies and changes — continues to rise in support of ensuring high-quality digital experience.

Interest and investment will continue to rise due to:

- Rapid growth in data volumes generated by the IT systems, networks and applications
- Increasing data variety — velocity at which data is generated and changing
- Challenges in maintaining observability and improving engagement due to the adoption of cloud-native and ephemeral architectures
- The need to intelligently and adaptively drive the automation of recurring tasks and predict change success and SLA failure

AIOps capabilities have evolved across multiple dimensions:

- The domain-agnostic AIOps platforms with vendors offering a general-purpose AIOps platform.
- Domain-centric AIOps vendors, that have the key components, but with a restricted set of use cases focused on one domain (for example, network, endpoint systems, APM or ITSM).
- Do it yourself (DIY), where end users can mix and match the components, essentially assemble tools for data ingest, a big data platform, ML and a visualization layer from multiple providers or open-source projects.

Machine learning uses multiple analytical approaches, while remediation requires significant maturity. Gartner still sees event correlation as the predominant practical use case, while aspirational goals like real-time business insights requires end-users to invest in resources like time, effort and skills. Remediation is still being handled via rule-based approaches although vendors are beginning to deliver ways to systemize and recall the problem resolution process for later reuse.

***User Advice:*** I&O leaders must build a strategic AIOps platform investment plan that is tied to driving measurable business outcomes though analysis of performance, digital experience and delivery automation while utilizing stagewise implementation of AIOps capabilities:

- Begin with practical goals, such as reducing operational noise through event correlation and anomaly detection, and later moving on to root-cause analysis.
- Start proactively detecting the signals that indicate emerging problems before users are impacted.
- Use NLP to democratize the automation of reoccurring workflows, making it easier to initiate them without deep specialist skills.
- Apply the pattern-matching capabilities of AIOps to the DevOps build-deploy process in order to detect potential impacts to production prior to deployment.

The AIOps strategy must account for the following:

- Balancing ease of implementation/use with interchangeability of platform capabilities
- ITOM tool portfolio rationalization
- Key technology gap investment

Before embarking on an AIOps journey, I&O leaders must determine whether using a domain-centric AIOps solution such as a monitoring tool that leverages machine learning is sufficient or whether a separate AIOps solution is necessary for their use cases. The domain-centric solution will likely have a shorter time to value, but its scope will be narrow and impact will be less. Domain-agnostic solutions may address a broad scope, and while their time to value will necessarily be longer their impact can be greater. If a domain-centric solution is already deployed for its primary purpose, evaluate its capabilities for AIOps in relation to the data sources that must be analyzed before considering a domain-agnostic solution.

***Business Impact:*** By enabling I&O teams to enhance and transform major operational functions with a real, automated insight generation capability, organizations across all verticals stand to realize:

- Agility and productivity gains — via active combined analysis of both IT and business data, yielding new insights on user interaction, business activity and supporting IT system behavior.
- Service improvement and cost reduction — via a significant reduction in time and effort required to identify the root cause of availability and performance issues. Behavior-prediction-informed forecasting can support resource optimization efforts.
- Risk mitigation — via active analysis of monitoring, configuration and service desk data identifying anomalies from both operations and security perspectives.
- Competitive differentiation/disruption — via superior responsiveness to market and end-user demand based on machine-based analysis of shifts, beyond those that are immediately obvious to human interpretation.

***Benefit Rating:*** Transformational

***Market Penetration:*** 5% to 20% of target audience

***Maturity:*** Emerging

***Sample Vendors:*** Aisera; Appnomic; BigPanda; BMC; Digitate; Moogsoft; ScienceLogic; ServiceNow; Splunk; StackState

***Recommended Reading:*** "Market Guide for AIOps Platforms"

"Avoid the Unexpected Consequences of IT Change Management With AIOps and CMDB"

"Assess Approaches to AIOps for a Comprehensive Solution"

"Deliver Cross-Domain Analysis and Visibility With AIOps and Digital Experience Monitoring"

"Augment Decision Making in DevOps Using AI Techniques"

## Programmable Infrastructure

***Analysis By:*** Nathan Hill; Philip Dawson; Milind Govekar

***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. It is also referred to as "infrastructure as code."

***Position and Adoption Speed Justification:*** Programmable infrastructure comprises a composable set of programmable building blocks. Programmable infrastructure goes beyond "aaS" (as a Service) offerings that expose programmable interfaces and enable new ways for delivering

infrastructure services. Programmable infrastructure strategies can be applied to private cloud, hybrid cloud and infrastructure platforms, as well as public cloud. Its goal is managing the life cycle of infrastructure delivery from provisioning, resizing and reallocation to reclamation, or in the case of elastic external resources, the termination of consumption.

APIs provide programmatic access to I&O services and data (e.g., depending on the workload requirements, an API that fires off automation that sets up a compute environment with CPU, memory and storage; installs software; assigns IP addresses). These are implemented so that I&O consumers (such as developers) can consume services and data to create new business solutions. Thus, I&O staff should be trained in using web technologies (such as HTTP and JSON) to develop these APIs. I&O leaders also should manage APIs as a technology product and implement full life cycle management, including version control and roadmaps.

The maturity of APIs that enable integration across different infrastructure platforms, combined with the scarcity of programmatic skills within I&O, account for the current maturity of programmable infrastructure.

***User Advice:*** Organizations cannot simply apply automation to existing monolithic infrastructure components. Doing so will result in frustration due to the awareness of agility and response demands without fundamental infrastructure components to deliver on requirements — in essence, automation without platform agility.

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 organizationwide 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.

Moving to an API-driven infrastructure is the key first step to enabling anti-fragile and sustainable automation through programmatic techniques. Achieving platform agility is not just about refreshing data center infrastructure to modern platforms like HCIs, although this may form part of the strategy. I&O leaders should consider all areas of the platform — cloud-native architectures, public and private cloud, new infrastructure for new products and services, as well as the modernization of legacy infrastructure.

***Business Impact:*** A continuous-delivery approach requires continuous insight and the ability to automate application responses. This ensures that (only) the right infrastructure resources are available at the right time and location, and this is achieved through a programmable infrastructure. Thus, programmable infrastructure ensures optimal resource utilization while driving cost-efficiencies. However, 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.

***Benefit Rating:*** High

***Market Penetration:*** 1% to 5% of target audience

***Maturity:*** Embryonic

***Sample Vendors:*** Alibaba Cloud; Amazon Web Services (AWS); Google; IBM; Microsoft; Pivotal; Tencent Cloud; VMware

***Recommended Reading:*** "Digital Platforms Need Programmable Infrastructure"

## Immutable Infrastructure

***Analysis By:*** Steve Riley

***Definition:*** Immutable infrastructure is not a technology capability, rather it is a process pattern in which the system and application infrastructure, once instantiated, is never updated in place. Instead, when changes are required, the infrastructure is simply replaced. Immutable infrastructure could encompass the entire application stack, with in-versioned templates provisioned via APIs, which are most commonly available in cloud IaaS and PaaS.

***Position and Adoption Speed Justification:*** Immutable infrastructure is typically used by organizations that take a DevOps approach to managing cloud IaaS or PaaS; however, it can be used in any environment that supports infrastructure as code. It represents a significant change in process for traditional infrastructure and operations groups. It may manifest as:

- Native cloud capabilities, such as Amazon Web Services (AWS) CloudFormation or Microsoft Azure Resource Manager templates
- Cloud management platforms, such as Flexera
- Software tools, such as HashiCorp's Terraform
- The customer's own automation scripts

Some or all of an application stack will be instantiated in the form of virtual machine images or containers, combined with continuous configuration automation tools that run after initial boot. Containers can be quickly replaced during runtime, while VM replacement is slower and requires greater coordination among other workload components. Containers improve the practicality of implementing immutable infrastructure and will drive greater adoption.

***User Advice:*** Immutable infrastructure ensures that 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. Cloud-native workloads are more suitable for immutable infrastructure architecture than traditional on-premises workloads. And, because redundancy may be required by CSP terms of service to receive service-level agreement relief, workloads designed with an immutable infrastructure approach lend themselves to easier replication.

The application stack for immutable infrastructure is typically composed of layered components, each of which should be independently versioned and replaceable. The base OS for the master image may be updated using traditional patching tools, or automatically or manually updated. Automation is then used to bundle components into artifacts suitable for atomic deployment, including VM images, container images, storage objects, network connections, and other necessary resources. The scripts, recipes, and other code used for this purpose should be treated similarly to the application source code itself, which mandates good software engineering discipline.

Some organizations that use immutable infrastructure reprovision only when a change is necessary. Others automatically refresh the infrastructure at frequent intervals (known as systematic workload reprovisioning) to eliminate configuration drift, to update components in which vulnerabilities were discovered, or to possibly eliminate advanced persistent threats. Frequent refresh is only practical in environments with fast and reliable provisioning; thus, it benefits strongly from containers. Integrate with a ticketing system so that refreshes can be initiated and tracked to completion.

The use of immutable infrastructure requires strict operational discipline. IT administrators should eliminate the habit of making one-off or ad hoc modifications to avoid configuration drift. Updates must be made to the individual components, versioned in a source-code-control repository, then redeployed so that everything is entirely consistent. No software, including the OS, is ever patched in production. Organizations that use immutable infrastructure may turn off all normal administrative access to instantiated compute resources — for example, not permitting SSH or RDP access. IT leaders should set a hard date for when all new workloads will use immutable infrastructure if technically feasible; deadlines can be effective motivators of behavior change.

None of the vendors listed in this innovation profile sell a product called “immutable infrastructure.” Rather, they offer one or more elements that help to establish an immutable infrastructure style. Expect to purchase multiple tools.

***Business Impact:*** Taking an immutable approach to server and compute instance management simplifies automated problem resolution by reducing the options for corrective action to, essentially, one. This is to destroy and recreate the compute instance from a source image containing updated software or configuration that addresses the problem. 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. In other words, getting to that single corrective action is not without effort. Treating infrastructure immutably is an excellent test of the completeness of your automation framework and the confidence of your platform. The immutable approach is a management paradigm, not a technology capability. The long-term outcome is one in which the workload defines the infrastructure, which is the opposite of traditional scenarios.

***Benefit Rating:*** Moderate

***Market Penetration:*** 5% to 20% of target audience

***Maturity:*** Adolescent

***Sample Vendors:*** Amazon Web Services; Ansible; Chef; Fugue; Google; HashiCorp; Microsoft; Puppet; SaltStack; Turbot

***Recommended Reading:*** "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"

"Solution Path for Infrastructure Automation"

"How to Make Cloud More Secure Than Your Own Data Center"

## Site Reliability Engineering

***Analysis By:*** George Spafford; Daniel Betts

***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). The site reliability engineer then collaborates with IT stakeholders to design and continuously improve systems that will meet the SLOs. For products or platforms that meet SRE guidelines, the engineer may choose to provide operational support.

***Position and Adoption Speed Justification:*** SRE is a discipline originally created by Google, and was described in the 2016 book, "Site Reliability Engineering: How Google Runs Production Systems." Adoption interest continues to grow both by digital-native organizations as well as traditional enterprises. SRE emphasizes the engineering disciplines that lead to resilience, but individual organizations implement SRE in widely varying ways. SRE is a complementary practice for organizations seeking to scale their DevOps activities.

SRE is intended to help manage the risks of rapid change, through the use of service-level objectives (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 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 enable organizational learning, continual improvement and reductions in unplanned work.

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), usage of infrastructure as code capabilities (which usually requires a cloud platform). SRE also uses automation to reduce manual processes, leverages resilient system engineering principles, and an agile development process that employs continuous integration/continuous deployment (CI/CD).

***User Advice:*** Organizations can benefit from SRE principles even if they are not sufficiently mature, agility-focused, or large enough to adopt SRE as a primary operations model. The SRE principles for risk management, release engineering, handling service-level objectives, monitoring, automation, and self-healing can be applied to a broader range of products and platforms. SRE also represents a useful means to scale DevOps initiatives.

An SRE initiative should have an executive sponsor. The first opportunity to begin with should have the following characteristics:

- The target application must change rapidly yet maintain high availability in order to maximize business value. Stakeholders should be politically friendly.
- The pilot must demonstrate sufficient value to improve credibility and support, yet also have an acceptable level of risk, allowing the stakeholders to learn.
- The initial SRE team must have a collaborative engineering mindset, strive to continuously learn and improve, and desire to automate tasks to reduce repetitious manual work, which is known as “toil.” It is often easiest to move DevOps-skilled employees from different parts of the organization, due to the relative difficulty of hiring engineers with SRE experience. A site reliability engineer is typically a software engineer with an excellent understanding of operations, or, less frequently, an infrastructure and operations engineer with strong programming skills.
- There must be clear SLOs that can be continuously monitored and reported against.
- The SRE collaborates with developers to help them learn how to design and build their product to meet the defined SLOs — the SRE is not doing the actual development work or inspecting quality in.
- The application development team must collaborate with the SRE team to meet SLOs. Developers are responsible for a resilient architecture and reliable code. SREs should not spend more than 50% of their time on ad hoc operational activities. Any excess should go to the developers for support.

An iterative approach must be used to start and evolve SRE practices. The teams involved must share experiences and lessons learned.

***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 in creation of new products or platforms that warrant the investment in reliability.

***Benefit Rating:*** Transformational

***Market Penetration:*** 5% to 20% of target audience

***Maturity:*** Adolescent

***Recommended Reading:*** "DevOps Teams Must Use Site Reliability Engineering to Maximize Customer Value"

"SRE and DevOps: End-to-End Accountability"

"Agile and DevOps Primer for 2020"

"Innovation Insight for Chaos Engineering"

"Maverick* Research: Software Testing and the Illusion of Exterminating Bugs"

## Infrastructure Automation

***Analysis By:*** Chris Saunderson

***Definition:*** Infrastructure automation (IA) tools allow DevOps and I&O teams to design and implement self-service, automated delivery services across on-premises and cloud environments. IA tools enable 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 an administration console.

***Position and Adoption Speed Justification:*** 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.

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
- Support for programmable infrastructure
- Self-service and on-demand environment creation
- Resource provisioning
- Configuration management

IA tools have become increasingly similar in the breadth of their configuration management content and enterprise capabilities. IA vendors are developing greater knowledge of configuration artifacts and state, activity patterns, roles, and policy. Vendors are leveraging these insights to prevent misconfigurations, resolve problems and provide more advanced deployment and optimization capabilities.

As IA tools are increasingly accepted by development and I&O groups, organizations are looking to replace their tribal implementations with an enterprisewide IA tool strategy.

***User Advice:*** Because IA tools provide a programmatic framework, the costs associated with them extend beyond just the licensing cost (or the lack thereof), so enterprises should include professional services and training requirements in cost evaluations. In particular, most I&O organizations should expect to invest in training because not all infrastructure administrators have the skills needed to use these tools successfully. IA tools have a learning curve, and it is tempting for developers and administrators to revert to known scripting methods to complete specific tasks. DevOps and IT operations leaders who want to maximize the value of IA tool investments must ensure that their organizations' culture can embrace IA tools strategically.

Use the following criteria to determine which IA vendor and product is appropriate:

- Internal IT skills
- Ecosystem surrounding IA tools
- Method for interacting with managed systems
- Security and compliance capabilities
- Authentication and authorization support
- Alignment to other tools within operating environment
- Orchestration functionality
- Scalability
- Platform and infrastructure content support

***Business Impact:*** By enabling infrastructure administrators and developers to automate the deployment and configuration of settings and software in a programmatic way, organizations across all verticals stand to realize:

- Agility improvements — By enabling continuous integration and delivery concepts to IT infrastructure management.
- Productivity gains — Via faster deployment and repeatable, version-controlled configuration of infrastructure.
- Cost-reduction improvements — Via significant reductions in required manual interactions by highly skilled and high-cost staff by automating "day 2" operational tasks. Licensing cost reductions may also be achieved.

- Risk mitigation — Compliance improves via the consistent use of standardized, documented processes and configurations across physical and virtual infrastructures.

IA tools can drive efficiencies in operational configuration management, as well as provide a flexible framework for managing the infrastructure of DevOps initiatives. They achieve this by integrating with other toolchain components — continuous integration (CI) and application release orchestration — in support of continuous delivery.

***Benefit Rating:*** High

***Market Penetration:*** 20% to 50% of target audience

***Maturity:*** Early mainstream

***Sample Vendors:*** Amazon Web Services (AWS); Chef; HashiCorp; Inedo; Microsoft Azure; Pulumi; Puppet; Quali; VMware

***Recommended Reading:*** "Market Guide for Infrastructure Automation Tools"

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

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

"How to Lead Digital Disruption With Programmable Infrastructure"

"Assessing HashiCorp Terraform for Provisioning Cloud Infrastructure"

## Application Release Orchestration

***Analysis By:*** Daniel Betts

***Definition:*** Application release orchestration (ARO) tools combine of 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.

***Position and Adoption Speed Justification:*** 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. The market has changed: the current landscape of vendors has built feature-comparable products, with some incremental differences. This poses a 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).

Demand for new applications and features delivered faster to support business agility continues to and will grow for the foreseeable future. As a result, the tumultuous and transformative activity

(often in the form of DevOps initiatives) that results 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.

***User Advice:*** Simplify and speedup the transition to automated workflows by prioritizing and documenting current application release procedures, activities and artifacts performed by both traditional and DevOps teams. Organize activities into three main categories that align with ARO vital capabilities: deployment automation, pipeline and environment management, and release orchestration. Prioritize capabilities according to your current and future needs prior to evaluating vendor offerings. The better understanding you have of your current release activities (especially where they are done manually), the faster you are likely to see value from any ARO tool.

When evaluating ARO tools, features should remain the No. 1 driver for selection of vendors to evaluate. Requirements should be mapped to vendor capabilities as a part of the evaluation process and ongoing assessment of fit should be encouraged. Where legacy environments (most cases, legacy — older tech stacks, some cases, first-generation client products) are in place, those features should be weighted more heavily than others. Vendors continue to improve overall dashboard delivery of not only release performance, but also the underlying platforms metrics — code deployment cycles, lead time from commit to deploy, incident recovery, change failure rate — and the contributing factors that drive them.

Areas of future opportunity exist to incorporate evolving needs into ARO platforms: value stream mapping, AI Ops, software delivery management and DevSecOps. While many ARO purchases are built around supporting a modern enterprise release management capability, just as many successful ARO implementations started with a focus around a specific platform, application or team, extending their value to others.

***Business Impact:*** 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 — Via faster delivery of new applications and updates in response to changing market demands
- Cost reduction — Via a significant reduction of manual interactions by high-skill and high-cost staff, freeing them to work on higher-value activities
- Risk mitigation — Via the consistent use of standardized documented processes and configurations across multiple technology domains
- Improvement and remediation — Via use of dashboard views over metrics outlining and predicting release quality and throughput

ARO tools provide transparency improvements to the release management process by making visible bottlenecks and wait states in areas such as infrastructure provision 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 delivered more quickly and reliably.

***Benefit Rating:*** High

***Market Penetration:*** 20% to 50% of target audience

***Maturity:*** Early mainstream

***Sample Vendors:*** Broadcom (CA Technologies); Chef; CloudBees (Electric Cloud); Digital.ai; GitLab; IBM (UrbanCode); Microsoft

***Recommended Reading:*** "Magic Quadrant for Application Release Orchestration"

"Critical Capabilities for Application Release Orchestration"

"How to Build and Evolve Your DevOps Toolchains"

## Cloud Data Backup

***Analysis By:*** Jerry Rozeman; Chandra Mukhyala; Michael Hoeck

***Definition:*** Policy-based, cloud data backup tools back up and restore production data generated natively in the cloud. The data can be generated by SaaS applications (e.g., Microsoft Office 365 or Salesforce) or by infrastructure as a service (IaaS) compute services (e.g., Amazon Elastic Compute Cloud [Amazon EC2] instances). Backup copies can be stored in the same or a different cloud location, or on-premises in the data center, where restore/recovery options should be offered in terms of restore granularity and recovery location.

***Position and Adoption Speed Justification:*** Backup of data generated natively in public cloud is an emerging requirement, because 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 they lack secure access control and consistent recovery points to recover from internal and external threats.

As Microsoft Office 365 (O365) gains more momentum, O365 backup capabilities have begun to emerge from mainstream backup vendors and small vendors. IaaS data backup, on the other hand, is a more nascent area that caters to organizations' need to back up production data generated in the IaaS cloud. Native backup of IaaS usually resorted to snapshots and scripting, which may lack application consistency, restore options, data mobility, storage efficiency and policy-based automation. However, more data center backup vendors now offer improved cloud storage backup capabilities that automate snapshot management and address some cloud-native limitations.

***User Advice:*** Before migrating critical on-premises applications to SaaS or IaaS, organizations need a thorough understanding of cloud-native backup and recovery capabilities and should compare them to their situations today. If the native capabilities seem to fall short (e.g., in application consistency, security requirements and recovery point objective [RPO]), factor additional backup costs into the total cost of ownership (TCO) calculation before migrating to the cloud. Organizations planning to use cloud-native recovery mechanisms should ensure that their contracts with cloud

providers clearly specify the capabilities and costs associated with the following items in terms of native data protection:

- **Backup/restore methods —** This describes how user data backup and restore are done, including any methods to prevent users from purging their own "backup copies" and to speed up recovery after a propagated attack, such as ransomware.
- **Backup/restore performance —** Some users have observed poor recovery time objectives (RTOs) when restoring or recovering data from cloud object storage.
- **Retention period —** This measures how long cloud providers can retain native backups free of charge or with additional cost.
- **Clear expectations in writing, if not service-level agreement (SLA) guarantees, regarding recovery time objectives —** RTO measures how long it takes to restore at different granular levels, such as a file, a mailbox or an entire application.
- **Additional storage cost due to backup —** Insist on concrete guidelines on how much storage IaaS's native snapshots will consume, so that organizations can predict backup storage cost.

For third-party backup tools, focus on ease of cloud deployment, policy automation for easy management, data mobility, storage efficiency and flexible options in terms of backup/recovery granularity and location.

***Business Impact:*** As more production workloads migrate to the cloud (in the form of SaaS or IaaS), it has become critical to protect data generated natively in the cloud. Deploying data protection for cloud-based workloads is an additional investment; however, this is often an afterthought, because it was not part of the business case. Without additional protection of cloud-based data, customers face additional risks, due to the impact of data loss, data corruption or ransomware attacks on their data.

SaaS and IaaS providers typically offer infrastructure resiliency and availability to protect their systems from site failures. However, when data is lost due to their infrastructure failure, the providers are not financially responsible for the value of lost data, and provide only limited credit for the period of downtime. When data is lost to user errors, software corruption or malicious attacks, user organizations are fully responsible themselves. The more critical cloud-generated data is, the more critical it is for users to provide recoverability of such data.

***Benefit Rating:*** Moderate

***Market Penetration:*** 5% to 20% of target audience

***Maturity:*** Emerging

***Sample Vendors:*** Actifio; Cohesity; Commvault; Dell EMC; Druva; Rubrik; Spanning Cloud Apps; Veeam; Veritas Technologies

***Recommended Reading:*** "Adopt Microsoft Office 365 Backup for Damage Control and Fast Recovery After Malicious Attacks"

"Debunking the Myth of Using EFSS for Backup"

## Container Management

***Analysis By:*** Dennis Smith

***Definition:*** Container management supports the management of containers at scale. This category of software includes container runtimes, container orchestration and scheduling, resource management and other container management capabilities. 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. It can also be used to more efficiently package COTS applications.

***Position and Adoption Speed Justification:*** Gartner surveys show that the demand for containers continues to rise. This is likely due to the growing adoption of container runtimes, which have introduced common container packaging formats that are more easily consumable by, and useful to, application developers and those with a DevOps approach to IT operations. Container runtimes, frameworks and other management software have increased the utility of containers by providing capabilities such as packaging, placement and deployment, and fault tolerance (e.g., cluster of nodes running the application). The emergence of de facto standards (e.g., Kubernetes) and offerings from the public cloud providers are also driving adoption. Container management integrates these various elements to simplify deploying containers at scale. Many vendors enable the 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 for that purpose.

The most common use of containers is focused specifically on Linux environments, and management software follows accordingly; however, there has been a gradual adoption of Windows containers. Container-related edge computing use cases have also increased, along with deployments involving bare-metal servers and the emergence of operational control planes that support containers and VMs.

Among the functionalities that container management systems provide are orchestration and scheduling, monitoring and logging, security and governance, registry management, and links to CI/CD processes. Among the vendor offerings are hybrid container management software, public cloud IaaS solutions specifically designed to run containers and PaaS frameworks that have incorporated integration with container management software. All major public cloud service providers are now deploying on-premises container solutions.

There is a high degree of interest in, and awareness of, containers within global organizations. Though many enterprises are planning or have recently commenced container deployments, few have containerized a significant portion of their application workloads. Additionally, there is significant grassroots adoption from individual developers who use containers with increasing frequency in development and testing — particularly for Linux. Container management software has progressed from an early-adopter technology to adolescent, where it remains.

***User Advice:*** Organizations should begin exploring container technology as a means for packaging and deploying applications and their runtime environments. Depending on the environment, container management tools are often deployed complementarily with continuous configuration management tools. As container integration is added to existing DevOps tools and to the service offerings of cloud IaaS and PaaS providers, DevOps-oriented organizations should experiment with altering their processes and workflows to incorporate containers. An organization may be a good candidate if it meets the following criteria:

- It's DevOps-oriented or aspires to become DevOps-oriented.
- It has high-volume, scale-out applications with a willingness to adopt microservices architecture, or has large-scale batch workloads.
- It has aspirational goals of increased software velocity and immutable infrastructure.
- It intends to use an API to automate deployment, rather than obtaining infrastructure through a self-service portal.

Organizations must also factor in their desire for hybrid and/or multicloud deployments into vendor selection, as many vendors offer container management software that can be deployed in different cloud environments.

***Business Impact:*** Container runtimes make it easier to take advantage of container functionality, including providing integration with DevOps tooling and workflows. Containers provide productivity and/or agility benefits, including the ability to accelerate and simplify the application life cycle, enabling workload portability between different environments and improving resource utilization efficiency and more. Container management software simplifies the art of achieving scalability and production readiness, and optimizes the environment to meet business SLAs.

***Benefit Rating:*** High

***Market Penetration:*** 20% to 50% of target audience

***Maturity:*** Adolescent

***Sample Vendors:*** Amazon Web Services; Google Cloud Platform; IBM; Microsoft Azure; Mirantis; Rancher Labs; Red Hat; VMware

***Recommended Reading:*** "Best Practices for Running Containers and Kubernetes in Production"

"Market Guide for Container Management"

"Best Practices to Enable Continuous Delivery With Containers and DevOps"

## Network Automation

***Analysis By:*** Josh Chessman; Andrew Lerner

***Definition:*** Network automation tools automate the configuration, visibility, troubleshooting, reporting and maintenance of physical and virtual network devices, and services. Network

automation tools can increase agility and operational efficiency, lower costs, reduce human error, and improve compliance with configuration policies.

***Position and Adoption Speed Justification:*** Based on interactions with clients and confirmed via conference polling, network automation often ranks as a No. 2 priority with networking teams in terms of strategic investment. "Network automation" is the sixth most-searched term among networking technologies considered for Gartner Hype Cycle, which is a composite metric based on Gartner search, Gartner Inquiry, and Google Trends. Further, network vendors are now embedding automation into nearly all management suites and it is becoming a baseline capability in markets such as SD-WAN. There are independent third-party tools that work across vendors that are also growing in popularity. Most organizations are using some form of network automation in production today, however, the depth of usage is limited. We estimate that roughly 30% of network changes are automated today with that number increasing to 50% in 2023. The overall market growth remains positive as the technology continues to move past the Peak, with Gartner estimating growth across all aspects of the market.

The discipline is held back partly by a lack of organizational process maturity pushing teams toward taking a pragmatic approach to resolving their organizations' specific requirements. This has frequently resulted in a cultural reluctance to adopt DevOps tools and principles as these promote agility while NetOps is focused on reliability and uptime. While a lack of scripting skills has been a barrier in the past, many tools have moved beyond basic scripting requirements which will lead to broader adoption of network orchestration tools.

***User Advice:*** We recommend:

- Measure, reward and socialize network automation within your organization by targeting business outcomes, such as faster service delivery, improved application availability or reduced operational expenses.
- Implement network automation in a gradual fashion by focusing on new network build-outs (both on-premises and cloud based) and non-change activities first, such as reporting and troubleshooting, and then establishing a baseline and evolving toward more critical activities.
- Invest in personnel by shifting the hiring and training focus away from hard network skills and toward those with more flexible skill sets, including coding (in a language such as Python) and familiarity with deployed or identified automation solutions. Additionally, cross-pollinating networking teams with adjacent DevOps personnel will be useful due to the significant overlap in skills and processes.

***Business Impact:*** Network automation tools can lower cost and improve operational agility. Consider network automation tools as components of a broader automation strategy. This demands participation in strategic, companywide deployment and configuration automation strategies (which are usually implemented as part of an IT service support management toolset), and integration with configuration management tools for other technologies, such as servers and storage.

***Benefit Rating:*** High

***Market Penetration:*** 20% to 50% of target audience

***Maturity:*** Early mainstream

***Sample Vendors:*** Apstra; BMC; Cisco; CloudGenix; NetBrain; Red Hat; SaltStack; SolarWinds; VMware

***Recommended Reading:*** "Jump-Start Network Automation to Scale Digital Initiatives"

"Cool Vendors in Enterprise Networking"

"Market Guide for Network Automation"

"3 Ways to Improve Network Automation"

"NetOps 2.0: Embrace Network Automation and Analytics to Win in the Era of ContinuousNext"

## Sliding Into the Trough

### Composable Infrastructure

***Analysis By:*** Daniel Bowers; Philip Dawson

***Definition:*** Composable infrastructure creates physical systems from shared pools of resources using an API. The exemplary implementation uses disaggregated banks of processors, memory, storage devices and other resources, all connected by a fabric. However, composable infrastructure can also aggregate or subdivide resources in traditional servers or storage arrays.

***Position and Adoption Speed Justification:*** Servers, storage and fabrics are traditionally deployed as discrete products with predefined capacities. Individual devices, or set amounts of resources from individual devices, are connected together manually and dedicated to specific applications. Composable infrastructure allows resources to be aggregated through software-defined intelligent automation, enabling infrastructure and operations leaders to achieve higher resource utilization and faster application deployment. Although some blade-based server infrastructures have long included composable networking features, composable infrastructure describes a broader spectrum of capabilities including disaggregation of accelerator, memory and storage resources.

Current 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 2020; for example, an agreement between next-generation fabric consortia, Compute Express Link (CXL) and Gen-Z Consortium, to cooperate on standards. A key step in the maturity timeline for composable infrastructure will be technology that can disaggregate DRAM from compute.

***User Advice:*** The deployment of composable infrastructure is appropriate where infrastructure must be resized frequently, or where composability increases the utilization of high-cost components. The majority of current use cases are in multitenant environments where composability allows 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.

Don't replace existing infrastructure to obtain composable infrastructure unless you have sufficient mature automation tools and skills to implement composable features. Verify that your infrastructure management software supports composable system APIs, or that you have the resources to write your own management tools. However, don't avoid infrastructure with composable features. Rather, don't choose such infrastructure *because* of those features unless you are prepared to use them.

***Business Impact:*** 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 in multitenant environments. However, a proliferation of vendor-specific APIs and the lack of off-the-shelf software for managing composable systems are headwinds to widespread adoption.

***Benefit Rating:*** High

***Market Penetration:*** 1% to 5% of target audience

***Maturity:*** Adolescent

***Sample Vendors:*** Dell Technologies; DriveScale; GigaIO; Hewlett Packard Enterprise (HPE); Intel; Liqid; Western Digital

***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"

## Intelligent Automation (I&O)

***Analysis By:*** Chris Saunderson

***Definition:*** Intelligent automation 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 collecting and analyzing data gathered from both human inputs and machine-based sources, and making recommendations or taking actions. Intelligent automation (IA) is increasingly being used for predictive and prescriptive analytics to improve operational efficiency and business agility, and is enabling technology for hyperautomation benefits.

***Position and Adoption Speed Justification:*** 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.

Current applications of AI-based automation are still narrowly focused on specific functional areas or specific operations. Intelligent automation, although transformative, is immature and highlights the difficulty in automation implementation unless the buyer uses a managed service provider; in that case, the MSP provides considerable benefit. One of the top technology challenges when it comes to leveraging AI techniques (such as ML and DNNs) for intelligent automation is the volume of data collected, the complexity of that data and the analytics associated with specific use cases. Although intelligent automation tool providers provide the underlying algorithmic implementations, connectors and data repositories, the implementation still requires significant setup and refinement, and is never "out of the box." The efforts to implement intelligent automation will require a high degree of cooperation between lines of business, I&O, and data and analytics teams, as well as technology providers.

Technology providers that offer best-of-breed tools for AIOps and RPA will influence intelligent automation. It is possible that AIOps and stand-alone RPA technology providers expand their offerings to deliver intelligent automation either through acquisitions or organic development. In many cases, infrastructure managed service providers white label third-party intelligent automation 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.

***User Advice:*** We recommend to:

- Define use cases before deploying IA by analyzing gaps in automation that benefit greatly from augmented decision making. However, note that the use of AI techniques as part of delivering IA is still nascent and in its early phases of maturity.
- Collaborate with data and analytics teams to adapt best practices that include data preparation, data cleansing and potentially building data lakes to glean insights from a centralized knowledge repository.
- Construct a data model that incorporates multiple variables that can be used to train AI models to suggest next actions. For most organizations, intelligent automation will be an evolutionary step in their automation maturity journey and therefore human intervention will be necessary during initial implementation, and development of skills to determine root cause for AI-derived exceptions will be key.
- Leverage existing investments in infrastructure managed service providers that offer (bundled) intelligent automation solutions or partner with stand-alone IA tool providers. Managed service providers represent the most common route to market for intelligent automation today.

- Incorporate intelligent automation as part of existing processes or redefined workflows to leverage AI models trained from a corpus of existing procedures and documentation.

***Business Impact:*** Intelligent automation can be applied to augment decision making in areas such as:

- Demand forecasting for infrastructure capacity
- Automated incident response (root cause analysis, event anomaly detection and automated response execution)
- Business process management (e.g., claims processing and document matching)
- Predictive capabilities (maintenance and failure effects and forecast need)

The journey to digital business requires I&O teams to advance in lockstep with business requirements. I&O leaders recognize that merely improving process efficiency through automating manual and repetitive activities will not result in competitive advantage. Hence, intelligent automation is aimed at improving the accuracy of decisions within complex workflows, and expanding the scope of automated workflows to enable new and differentiated business value.

Traditionally, the process of collecting and updating data for capacity planning forecasts, asset utilization and cost optimization has largely been manual. This is a challenge for I&O leaders because it is neither up to date nor accurate and thus results in flawed decisions. I&O leaders are looking to intelligent automation as an engine that continually collects and updates data models with the ability to predict business outcomes and automate or augment business decisions based on the data.

***Benefit Rating:*** High

***Market Penetration:*** 1% to 5% of target audience

***Maturity:*** Emerging

***Sample Vendors:*** arago; AutomationEdge; Ayehu; BMC (TrueSight); Cortex; CSS Corp; HCL Technologies; IPsoft; TCS

## Continuous Delivery

***Analysis By:*** Hassan Ennaciri

***Definition:*** Continuous delivery (CD) is an approach that enables DevOps teams to create an automated pipeline for producing software in short cycles. CD ensures that software can be reliably released any time via a DevOps toolchain and is a key capability of a DevOps initiative.

***Position and Adoption Speed Justification:*** Growing DevOps initiative success continues to drive enterprise investments in CD capabilities. CD improves release velocity and reliability while simplifying compliance enforcement via automation. Continuous integration (CI), automation and testing are core to CD. These functions provide environment models that can be leveraged

throughout the software development life cycle (SDLC) to more consistently deploy application builds and updates.

CD is a nonprescriptive, evolving approach that DevOps teams can deliver and realize in many ways. Given the emerging state of CD, market demand and vendor responses have been fragmented. DevOps teams typically start by automating functions that can clearly demonstrate the value of CD (e.g., application deployment and release configuration) when integrated with CI and testing. As a logical linkage between CI and operational functions, CD plays a critical role in building scalable DevOps toolchains.

***User Advice:*** DevOps teams should incorporate CD processes to help reduce friction throughout the SDLC. They must also evaluate and invest in associated tooling, such as application release orchestration tools, containers and continuous configuration automation tools. These tools provide some degree of environment modeling and management, which can prove invaluable for scaling CD capabilities across multiple applications.

When starting a CD initiative, enterprises must consider all associated technologies and take an interactive 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 proficiency metrics. DevOps product teams should assume that there will be continual discoveries about roles and responsibilities, required skills, automation details and documentation, especially during the early phases of adoption. DevOps teams should build requirements for CD tools with a broader view than just one environment (development, test, quality assurance, preproduction or production) and one application (for example, Java and .NET). The primary application of CD is to extend CI processes, but organizations also need to consider applying CD principles to infrastructure automation.

***Business Impact:*** CD is a key capability of 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.

***Benefit Rating:*** High

***Market Penetration:*** 20% to 50% of target audience

***Maturity:*** Adolescent

***Sample Vendors:*** Broadcom; Chef; CloudBees; GitLab; Harness; IBM; Microsoft; Puppet

***Recommended Reading:*** “How to Build and Evolve Your DevOps Toolchains”

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

“Magic Quadrant for Application Release Orchestration”

"Critical Capabilities for Application Release Orchestration"

## Software Asset Management Tools

***Analysis By:*** Ryan Stefani

***Definition:*** Software asset management (SAM) tools help maintain compliance with licensing agreements and optimize software spending by identifying opportunities to reuse software, by monitoring consumption and providing data to improve software negotiations. They facilitate this by aggregating organization's entitlement and consumption data, and then reconcile it in order to establish an effective license position (ELP). This is becoming increasingly important given the complexity of SAM in hybrid environments.

***Position and Adoption Speed Justification:*** While SAM tools continue to be of interest within organizations to simplify the management of their software in order to reduce waste and risk of noncompliance, they've come to find that SAM tools alone do not suffice. Organizations that have opted to procure, deploy and maintain a SAM tool have encountered issues with realizing the expected benefits, leading to failed SAM initiatives.

This disappointment is attributed to two key factors:

- **Underestimating complexity of managing entitlements.** Most software obtained by organizations does not comply with ISO 19770-3 format, which provides data and format structures for publishers to provide customers with once they purchase entitlement to enable automated loads of software entitlements. This results in a complex and resource-intensive process to manually enter their software entitlements that is often overlooked at the time of purchase.
- **Inability to automatically create an ELP.** SAM tool vendors market their solutions' ability to easily produce an ELP for complex licensing. While SAM tools do enable easier ELP creation, the increasing complexity of environments and license metrics often inhibit the ability to automate this process. The core means for identifying software consumption to support reconciliation, is through the use network discovery and inventory tools. This does prove valuable for many software applications but doesn't account for alternative metrics that aren't discoverable such as indirect access or client access. This leads to manual intervention, or the use of additional data collection tools to produce an ELP.

While SAM tools don't fully automate the management of software, they help organizations automate portions of the function. This is still extremely valuable as it reduces the time required to manually produce an ELP and allows skilled resources to focus on identifying opportunities to optimize the software estate.

***User Advice:*** Determine what publishers, applications and environments are in scope. Focus on the most impactful publishers. Start with the top 80% of software spend and publishers with a high risk of audit activity. This list should be manageable and would concentrate your efforts based on the most significant impact.

From there, obtain a list of the underlying applications your organization uses to focus on three items:

- **Entitlement management:** Organizations should evaluate the vendors' product catalog for in-scope applications, to determine the level of effort required to create and maintain accurate entitlement records. Loading and managing entitlements is a resource-intensive process, that should be accounted for. Organizations can also look to third parties such as SAM service providers or resellers with licensing expertise to help with these ongoing efforts.
- **Consumption:** Determine how is consumption measured, per user, per install, hardware configuration, etc. Then ascertain what environments (IaaS, SaaS), operating systems, and virtualization technologies are present in the organization, as these will determine how consumption is measured and your inventory needs strategy. Use the out-of-the-box SAM tool integrations, where available, and constantly monitor data for accuracy and ensure that no new data is needed to monitor consumption. If needed, evaluate the use of additional data sources or tools required to supplement your SAM tool.
- **Reconciliation:** Don't anticipate having a real live ELP for all applications all the time. Organizations must create a schedule for reconciliation of in-scope applications, based on risk and events like renewals. Creation of an ELP is very resource-intensive and requires highly specialized expertise for specific publishers. Organizations must adequately staff for this effort or seek the assistance of third-party service providers to successfully create ELPs in order to optimize their costs.

***Business Impact:*** Software expenditures continue to grow and remain a top IT expense for most organizations. At the same time, software vendor audits are still prevalent, as they continue to underpin revenue; this is likely to disrupt organizations with unplanned expenditures. Additionally, 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.

SAM tools manage software licenses to help mitigate compliance risk and optimize consumption. All industries need to both reduce audit risk and optimize software spending. As organizations move to new licensing models, they must efficiently consume licenses to avoid creating high watermarks in their licensing agreements that will be a challenge to true-down after the fact. Procurement departments will benefit from SAM by having better data to support contract renewals and prevent license compliance issues that offset their negotiation leverage. Gartner expects strong, continued adoption among enterprises that want to implement software license management for compliance and improve spending for installed and as-a-service software.

***Benefit Rating:*** High

***Market Penetration:*** 5% to 20% of target audience

***Maturity:*** Adolescent

***Sample Vendors:*** Aspera; Certero; Eracent; Flexera; Ivanti; License Dashboard; Matrix42; ServiceNow; Snow Software; Xensam

***Recommended Reading:*** "Magic Quadrant for Software Asset Management Tools"

"Critical Capabilities for Software Asset Management Tools"

"Software Asset Management for the Cloud: Consumption Management and Optimization Take Center Stage"

"Three Critical Elements of a Successful Software Asset Management Tool Implementation"

## DevOps Toolchain

***Analysis By:*** Thomas Murphy

***Definition:*** A DevOps toolchain comprises tools used to support DevOps pipeline activity and provide fast feedback. It has come to focus primarily on the code to cloud build/test/deploy sequence. Pipeline activities have started with discrete tools for various steps, but we are increasingly seeing vendors deliver solutions right across the application development and delivery cycle. The mix of tools is determined by business need, product platform, language, product domain and the skills of the people who will use the tools.

***Position and Adoption Speed Justification:*** DevOps toolchains emerge from the need to deliver new and changed applications faster. They can include dozens of unintegrated tools, which makes automation a technically complex and arduous task. But the biggest challenge facing organizations does not arise from the tools themselves, or their diversity, but rather from the belief that DevOps is achieved simply through tooling. Even if it is tooling, Gartner's DevOps survey found that organizations have, on average, 28 toolchains, which represents a large undertaking to create and maintain.

The market continues to evolve via acquisitions, the emergence of open-source and new commercial products, and the continued development of cloud architecture. Core tooling around CI 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 these core pipelines evolve, we also are seeing a new wave of "toolchains" that is broader and more encompassing emerging around value stream management. We expect organizations will have multiple toolchains of the pipeline variety and these will feed data into value stream tools.

***User Advice:*** We recommend that I&O and application leaders develop a toolchain strategy to establish business objectives, identify practices to achieve those objectives, and then select tools to support those practices. The selection of tools should be the last part of the process.

Software engineering practices such as version control, code management and managed distribution should be utilized. The toolchain should be focused on removing execution barriers and automating the development and continuous delivery process. Each DevOps product or platform

team member should understand the capabilities and contribution of each tool in the DevOps toolchain in order to avoid tool overlap, conflict and toolchain functionality gaps.

Remember that tools — even open-source ones — are not free. There is a cost attached to learning, integrating and (especially when they are integrated) replacing them.

Therefore DevOps leaders should:

- Expect to have more than one toolchain to support the different technology stacks and delivery platforms targeted (e.g., COTS, cloud, mainframe, container-native).
- Seek to utilize pipeline integrated security and compliance and focus on effective test automation.
- Establish a toolchain community of practice to help manage and evolve toolchains and monitor new technology developments.

***Business Impact:*** Delivering business value is central to DevOps. This requires a collaborative product team focused on delivering applications when the business demands them, which, in turn, demands an agile mindset and the technology to support the activity needs of individual team members. A well-designed, integrated and automated DevOps toolchain enables development and operations team members to work together, with common objectives and metrics, to ensure quality, on-time application delivery to the business.

***Benefit Rating:*** High

***Market Penetration:*** 20% to 50% of target audience

***Maturity:*** Early mainstream

***Sample Vendors:*** Amazon Web Services; Atlassian; CloudBees; Codefresh; GitLab; Harness; HashiCorp; Microsoft

***Recommended Reading:*** “The Future of DevOps Toolchains Will Involve Maximizing Flow in IT Value Streams”

“How to Build and Evolve Your DevOps Toolchains”

“Guidance for Securing the DevOps Toolchain With IAM”

“Ignition Guide to Managing a DevOps Toolchain”

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

## Intent-Based Networking

***Analysis By:*** Andrew Lerner

***Definition:*** An IBN system is a closed-loop system to help design, provision, and operate a network, based on business policies. IBNS is typically packaged as software and a full IBNS includes four key subcomponents:

- Can translate a higher-level business policy to a network configuration
- Can automate network activities across network components
- Has awareness of network state/health
- Provides continuous assurance and enables dynamic optimization

***Position and Adoption Speed Justification:*** IBNS is being hyped by networking vendors because of the promise to improve network availability and agility simultaneously, enabling digital business transformation. However, as of early 2020 real-world enterprise adoption of full IBNSs is nascent. We estimate fewer than 100 full deployments that meet all phases of the definition. The detailed description of the subcomponents of IBNS includes:

- **Translation and validation:** System can take a higher-level business policy (what) as input from end users and convert it to the required network configuration (how).
- **Automation:** System can configure appropriate network changes (how) across existing network infrastructure.
- **State awareness:** System ingests real-time network status for systems under its control.
- **Assurance and dynamic optimization:** System continuously validates that business intent is being met; can take corrective actions when it is not.

Each of the four subcapabilities of intent can be deployed independently. There is much heavier adoption of certain individual components, including automation. These components delivered individually add value, but are not full intent when they aren't delivered together as part of a closed loop.

In the last 18 months, the terminology around intent (including intent-based, intent-driven, IBN, etc.) has largely been taken over by vendor marketers, as there is rampant overmarketing of intent by networking vendors. Things such as automation, abstraction and programmability are described as intent. Unfortunately, many products are marketed by vendors as intent that falls short of the full capabilities of intent.

We anticipate that the number of full closed-loop IBNS commercial enterprise deployments to remain below 200 through 2020, and increase moderately by the end of 2021. We expect adoption to be pragmatic — associated with new build-outs and/or network refresh initiatives. Through 2020, early rollouts are likely to be in larger-scale environments for well-defined and specific use cases, such as spine/leaf data center networks. We expect that data center networking vendors will increasingly incorporate assurance, validation and dynamic remediation into their networking suites, getting closer to a full IBN.

We recommend and anticipate that adoption will be phased, with the different IBNS subcomponents enabled gradually over months and years. Technologically, IBNS requires the ability to abstract and model network behavior, which has proved difficult historically, particularly in multivendor environments. Furthermore, IBNS represents a substantial cultural shift in how networks are designed and operated, which will create barriers to adoption in many risk-averse enterprises.

***User Advice:***

- Deploy IBNS pragmatically in phases, because each of the four individual subcomponents adds value. For example, organizations can deploy an IBNS in "notify mode," whereby a skilled engineer must approve a proposed automated change suggested by the IBNS.
- Mandate support for open, RESTful APIs when purchasing new networking infrastructures to support integration within an IBNS moving forward.
- Choose an IBNS that supports multivendor network infrastructures and extends into public cloud environments to support a broader range of use cases and avoid vendor lock-in.
- Tune-out vendor marketing regarding products that are listed as intent.

***Business Impact:*** Gartner sees the biggest benefits from IBNS as improving network agility and availability, and supporting unified intent and policy across multiple infrastructures. When the technology matures, a full IBNS implementation can reduce the time to deliver network infrastructure services to business leaders by 50% to 90%, while simultaneously reducing the number and duration of outages by at least 50%. Although agility and availability are the high-level benefits, IBNS provides several other specific benefits, including:

- **Reduced operating expenditure (opex) —** Reduce opex associated with managing networks and free up senior-level network resources 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 —** Intent tools may circumvent the costs of other related network infrastructure tooling, because automation and orchestration are embedded in IBNS.
- **Better documentation —** IBNS provides real-time self-documentation, which also includes the rationale (intent) behind design/configuration decisions.
- **Improved compliance —** IBNSs simplify auditing, due to the algorithmic correctness of configurations, direct mapping to business intent and ongoing, dynamic, real-time validation.

***Benefit Rating:*** Moderate

***Market Penetration:*** Less than 1% of target audience

***Maturity:*** Emerging

***Sample Vendors:*** Apstra; Cisco; Forward Networks; Gluware; Huawei; Intentionet; Juniper Networks; NetYCE; VMware

***Recommended Reading:*** "Innovation Insight: Intent-Based Networking Systems"

"Cool Vendors in Enterprise Networking"

## Software-Defined Infrastructure

***Analysis By:*** Philip Dawson

***Definition:*** Software-defined infrastructure (SDI) includes the broad set of software-defined anything (SDx) infrastructure components and the software-defined data center (SDDC). SDI also includes non-data-center infrastructure deployed in Internet of Things (IoT) applications and an SD edge of edge-based adapters, monitoring devices, gateways, appliances and machines.

***Position and Adoption Speed Justification:*** Data center infrastructure is well-covered with 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. This 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. In 2020, we are seeing SDI move to vendor-specific silo technology (not heterogeneous service drive) and, hence, obsolete as multivendor interoperable standards.

***User Advice:*** As SDI initiatives roll out, consider the integration and measurement of non-data-center edge infrastructure. Focus on core IT SDI for compute, network, storage and facilities, but consider the impact of SDI on IoT, edge computing, remote office/branch office (ROBO) and other operational technologies. 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. Expect SDI to be tied to a specific vendor or technology silo.

***Business Impact:*** With the increase of IoT touching edge-based operational technology, SDI reaches beyond and between SDDCs, and leverages SDI benefits and features for new multimode applications and edge IoT endpoints. However, SDI is now tied to vendor technology not interoperability.

***Benefit Rating:*** High

***Market Penetration:*** 20% to 50% of target audience

***Maturity:*** Obsolete

***Sample Vendors:*** IBM; Intel; Microsoft; Red Hat; VMware; Wipro

***Recommended Reading:*** "Simplify Intelligent Infrastructure by Using Workload Architectures"

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

## Hybrid Cloud Computing

***Analysis By:*** David Smith; Milind Govekar

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

***Position and Adoption Speed Justification:*** 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. 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 (for example, cloudbursting).

Hybrid cloud computing is different from multicloud computing, which is the deliberate use of cloud services from multiple public cloud providers.

A hybrid cloud computing architecture complements multicloud computing. Although most organizations are integrating applications and services across service boundaries, we estimate approximately 15% of large enterprises have implemented hybrid cloud computing beyond this basic approach — and for relatively few services. This decreases to fewer than 10% for midsize enterprises, which mostly are implementing the availability/disaster recovery use case. 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 to customers building and managing an integrated hybrid IT operating model. These services are provided by vendors (such as Accenture, Wipro and TCS) and other service providers and system integrators.

Microsoft's Azure Stack Hub, Google's Anthos, VMware's hybrid cloud portfolio, and AWS's Direct Connect and Amazon Virtual Private Cloud (VPC) are all attempts to support hybrid cloud implementations. Red Hat's OpenShift and Pivotal Web Services are attempts to support hybrid PaaS implementations.

As more providers deliver hybrid cloud offerings, they are increasingly delivering 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.

***User Advice:*** 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 applications and services to form a hybrid environment. Approach sophisticated cloudbursting and dynamic execution cautiously, because these are the least mature and most problematic hybrid approaches. To encourage experimentation and cost savings, and to prevent inappropriately risky implementations, create guidelines/policies on the appropriate use of the different hybrid cloud models. 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. If your organization is implementing hybrid IT, then consider using hybrid cloud computing as the foundation for implementing a multicloud broker role and leveraging hybrid IT services and service providers to complement your own capabilities.

***Business Impact:*** Hybrid cloud computing enables an enterprise to scale beyond its data centers to take advantage of the elasticity of the public cloud. Therefore, it is transformational when implemented, 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), as these constituencies are also moving toward a hybrid cloud computing model.

***Benefit Rating:*** High

***Market Penetration:*** 5% to 20% of target audience

***Maturity:*** Adolescent

***Sample Vendors:*** Alibaba Cloud; Amazon Web Services (AWS); Google; Hewlett Packard Enterprise (HPE); IBM; Microsoft; Oracle; Rackspace; Red Hat; VMware

***Recommended Reading:*** “The State of Hybrid Cloud”

“Market Guide for Managed Hybrid Cloud Hosting, North America”

“Prepare for AWS Outposts to Disrupt Your Hybrid Cloud Strategy”

“Utilizing Hybrid Architectures for Cloud Computing”

“Top 10 Strategic Technology Trends for 2020: Distributed Cloud”

“I&O Leaders Must Plan for Hybrid Cloud Orchestration”

“Cloud Adoption Is Driving Hybrid WAN Architectures”

## Intelligent Automation for Infrastructure Managed Services

***Analysis By:*** David Groombridge; Stephanie Stoudt-Hansen

***Definition:*** Gartner uses the umbrella term "intelligent automation" to cover a variety of strategies and 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 synthesis, machine vision, and machine reasoning. Intelligent automation (IA) for infrastructure managed services is the application of these technologies to IT infrastructure operations, delivered through managed services.

***Position and Adoption Speed Justification:*** Infrastructure service providers continue to enhance their automation capabilities and embed IA deeper in their existing infrastructure services. Where service delivery relies on knowledge workers, IA can be used instead for routine parts of that work, reducing human effort, potential errors and thus cost. Within service desk provision, leading providers can use analytics capabilities to reduce the occurrence of incidents by 30% to 80% for some clients, and then resolve 15% to 25% of the remaining tickets without human intervention. In addition, global outsourcers can automate 80% to 95% of the provisioning and management of hybrid infrastructure services using tools that learn and automate the required operational activities. This automation is now extending further into related services such as application administration and security services.

Penetration of these services into enterprises is increasingly common but not yet universal, with existing contracts often seeing little change until renewal. Most leading infrastructure services providers now 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, spanning complex operational processes. 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. As such service providers continue to make substantial investments in these services, they will evolve rapidly and become core parts of all infrastructure service offerings within a few years.

***User Advice:*** 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, though, buyers should expect that savings will now be achieved by "automation arbitrage," in which intelligent automation replaces a substantial part of the human labor in provider offerings. In comparing providers' offers, sourcing, procurement and vendor management leaders should evaluate the use of intelligent automation in infrastructure managed services by seeking concrete pricing and quality commitments from service providers in the form of outcome-based contracts. In particular, with lower labor usage, an added benefit of higher quality from reduced errors should be reflected in ongoing improvements in contractual SLAs.

The critical component needed to make intelligent automation work is a substantial and detailed data record. For infrastructure managed services, AI systems will learn by tracking the actions of engineers during incident resolution, and by reading and identifying patterns in logs of incident, change or other data from the recent past, 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 to their organizations 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.
- 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.

***Business Impact:*** Intelligent automation in infrastructure managed services offers a number of potential benefits. Gartner expects contracts containing intelligent automation to show annual cost savings of 2% to 8% for commodity services, depending on the specific service and the extent of its use. Furthermore, it will become easier in the future for businesses to scale to new business demand by rapidly deploying new instances of intelligent automation rather than hiring new people. In addition, such intelligent automation will not require annual pay raises or additional hiring due to staff turnover. The intelligent nature of the automation also generates analytical insights that allow for proactive and preventative maintenance actions, to help reduce system downtime and impact to users. This combination of rapid scaling, multi-language, reduced business impact and repeatable quality that intelligent automation delivers, along with the ability to refocus remaining staff on more value-added business needs, in turn drives improved user satisfaction and SLA delivery.

***Benefit Rating:*** High

***Market Penetration:*** 5% to 20% of target audience

***Maturity:*** Adolescent

***Sample Vendors:*** Accenture; Atos; Cognizant; Fujitsu; HCL Technologies; Hexaware; IBM; Tata Consultancy Services; Tech Mahindra; Wipro

***Recommended Reading:*** “Market Guide for Intelligent Automation Leveraged for IT Managed Services”

“Scale Infrastructure Operations With Intelligent Automation and a Central Knowledge Unit”

## Climbing the Slope

### DevSecOps

***Analysis By:*** Neil MacDonald; Mark Horvath

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

***Position and Adoption Speed Justification:*** Originally proposed by Gartner in 2012, adoption of DevSecOps takes time, but interest is high. Several security vendors directly target DevSecOps use cases, and mainstream adoption is less than five years away. Slow rates of adoption and slow movement on the Hype Cycle are primarily due to the process and cultural changes required across IT organizational silos to adopt agile "DevOps like" models and to include security in this to deliver DevSecOps. However, industry initiatives around "secure DevOps," DevSecOps, DevOpsSec, and "rugged DevOps" have gained significant traction. Leading security vendors are evolving their solutions to become more programmable, laying the foundation for higher levels of automation and orchestration from testing into deployment.

DevOps (often combined with container/Kubernetes adoption and programmatic cloud infrastructure) is being driven by developers in the name of speed and agility. Security must be a part of this shift, but in a way that respects the collaborative nature of DevOps. Security cannot be siloed, which forces developers outside of their toolchain to perform security testing. DevSecOps offerings need to programmatically integrate with common CI/CD testing tools to support automation and without requiring a security professional to be involved — other than setting policy guiderails to be applied. In addition, the declarative nature of scripts and cloud automation tools used in development can be tied automatically to programmable security infrastructure for protection at runtime. Whether you drive security from container layers, scripts, templates or toolchains, the desired outcomes are the same — the automated and compliant configuration of the underlying security infrastructure based on policy, reflecting the intended state of the workloads.

***User Advice:*** Investigate the adoption of a DevSecOps operating model for next-generation data center infrastructure or public-cloud-based computing environments to automatically link security policy enforcement mechanisms with the deployment of new workloads. As your organization investigates DevOps operating models or moves toward more-agile IT development and operations processes, consider these actions:

- 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.
- Start identifying OSS components and vulnerabilities in development as a high-priority project (referred to as software composition analysis), as the biggest risk comes from known vulnerabilities and misconfigurations.
- Invest in programmable security infrastructure capable of supporting security policy toolchains, which facilitates speed through automation and flexibility via open APIs (typically, REST-based). 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 be capable of applying security policies in container and Kubernetes-based development and deployment environments.
- Experiment with DevSecOps workflows using public cloud infrastructure and programmatic ways that security policies can be integrated into templates, blueprints and recipes to avoid manual security policy configuration.
- Favor offerings that can link scanning in development (including containers) to correct configuration and protection at runtime.

***Business Impact:*** As IT development and operations processes become more agile (including shifts to DevOps operating models), security must not be an afterthought and should be seamlessly integrated into agile development processes — DevSecOps. 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.

***Benefit Rating:*** Transformational

***Market Penetration:*** 20% to 50% of target audience

***Maturity:*** Early mainstream

***Sample Vendors:*** Aqua Security; Contrast Security; Data Theorem; NowSecure; Palo Alto Networks; ShiftLeft; Snyk; Sonatype; Synopsys; Veracode

***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"

"How to Make Cloud More Secure Than Your Own Data Center"

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

## ITIL

***Analysis By:*** Mark Cleary

***Definition:*** ITIL is an ITSM framework owned by AXELOS, a joint venture between the U.K. Government and Capita. ITIL provides best practices, from a service perspective, in the definition, design, deployment and management of products and services delivered by IT to the business. Related activities are collated as 'practices' to address specific aspects of service delivery such as

managing incidents or changes, negotiating service levels or ensuring there is enough capacity in the infrastructure.

***Position and Adoption Speed Justification:*** ITIL is used to provide a consistent, repeatable and standardized approach to the planning and management of IT services. A successful implementation significantly improves the competence and capabilities of an infrastructure and operations (I&O) organization allowing it to move from a technology to a service focus.

Interactions with Gartner's clients show that more than 80% of I&O leaders use ITIL, but many state momenta has stalled usually due to a lack of governance, and cultural resistance from the change in working practices. This results in a reduction in the service quality due to a lack of compliance with the ITSM disciplines.

The ITIL 4 Foundation was published in 2019, but uptake appears to be low. ITIL 2011 remains the predominant implementation and is based on the service life cycle. However, most clients focus on the operational aspects rather than the strategy, design and transition components.

The mainstream adoption of ITIL has moved higher on the Plateau of Productivity due to its principle value to the production environment.

***User Advice:*** Organizations looking to upgrade to ITIL 4 should continue with their current journey, review the ITIL 4 publications and assess the impact of any upgrade.

ITIL should be leveraged as one source of good practice that must be refined to meet your specific business goals. While key developments, such as the rise in agile and DevOps practices, digital transformation, and changing landscapes (including cloud), are not reflected in ITIL 2011, they are addressed in ITIL 4. Review the ITIL 4 management practices for the latest thinking and seek additional inspiration in sources such as DevOps and agile methodologies.

ITIL helps put IT service management into a strategic context and provides guidance on service management practices and associated factors in the service life cycle. Leaders will be successful if they pragmatically leverage the advice in ITIL and other sources to transform their practices, culture and competence. For many this will require a review of their current approach to ensure that ITIL is adapted in line with agile thinking while remaining focused on business outcomes.

***Business Impact:*** ITIL can support I&O by having a significant impact on the business if it is implemented correctly. Defining and deploying practices that can be used across the organization in a consistent and standardized way improves the credibility of I&O and increases the business' confidence in IT's ability to deliver. Following an initial investment in the core practices of incident and change management, I&O leaders can better plan and manage their environment by investing in further ITIL practices that extend their service competence and capabilities. The benefit of this approach is an improvement in I&O's ability to deliver services and meet targeted business outcomes. New ways of working are also catered for as ITIL 4 provides advice and guidance on how to integrate ITIL practices with, for example, agile and DevOps frameworks.

***Benefit Rating:*** High

***Market Penetration:*** More than 50% of target audience

***Maturity:*** Mature mainstream

***Recommended Reading:*** "2019 Strategic Roadmap for IT Service Management"

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

"How to Organize IT for Efficiency"

"Product Planning Primer for 2020"

"Agile and DevOps Primer for 2020"

"Infrastructure, Operations and Cloud Management Primer for 2020"

## Cloud Application Discovery

***Analysis By:*** Jay Heiser

***Definition:*** Cloud application discovery (CAD) refers to mechanisms for security, licensing, compliance and I&O professionals, providing visibility into enterprise activity associated with the use of public cloud applications. CAD provides information on application name and type, and usage by individual and department. Ideally, an application discovery tool also provides information about the cloud service provider, including a risk rating.

***Position and Adoption Speed Justification:*** IT professionals are increasingly recognizing that the identification and analysis of unsanctioned IT are critical elements of data governance, cybersecurity and IT spend management, encouraging the utilization of CAD functionality. Regulations, especially the EU GDPR and CCPA, are providing additional incentive to determine what SaaS applications are being used in what way. Dozens of multifunction products offer different levels of CAD functionality, supporting different corporate IT roles. 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. The proliferation of CAD across so many different functions represents a confusing market, but it means that most IT departments already have some capability to identify "shadow IT," although many have not yet tried to apply this capability.

***User Advice:*** All organizations that are heavily regulated or have large amounts of critical data should be either controlling access to SaaS or monitoring SaaS usage through CAD mechanisms. As more enterprises put policies in place that require explicit risk acceptance decisions for the use of SaaS, they require mechanisms to identify unauthorized SaaS use and monitor authorized SaaS use to ensure it is meeting policies. The decision about when and where to place additional controls over the "virtual enterprise" represented by SaaS starts with tools that can report on the extent to which external applications are being utilized. This provides information in support of defensible decisions about the organizational use of SaaS, and will ensure that "unsanctioned IT" can be identified, helping organizations prioritize their SaaS risk assessment and control efforts.

CAD products differ in the sources used for collecting the data, which can come directly from the endpoints or, more conveniently, from firewalls or secure web gateways. They also differ in the level and form of information they report. The most useful CAD products provide some information that can help IT security, privacy, compliance and other IT governance functions to focus attention on the applications that are most likely to represent higher levels of risk.

***Business Impact:*** Most organizations have hundreds, even over 1,000, 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 discovery tools are useful in identifying this "unsanctioned IT," facilitating security, compliance, SaaS license management and even control over usage fees. Most organizations have some form of tool that includes a CAD function, but the majority of organizations still fail to fully apply this capability, thus complicating the estimate of market penetration. Gartner anticipates that visibility into cloud application usage will eventually be considered a mandatory function by auditors and regulators, but the level of urgency continues to be relatively low.

***Benefit Rating:*** Moderate

***Market Penetration:*** 20% to 50% of target audience

***Maturity:*** Early mainstream

***Sample Vendors:*** Censornet; Eracent; Flexera; McAfee; Microsoft; Netskope; Scalable Software; Snow Software; Symantec; Torii

***Recommended Reading:*** "Magic Quadrant for Cloud Access Security Brokers"

"How to Develop a SaaS Governance Framework"

"Solution Path for a SaaS Adoption Framework"

## Cloud Management Platforms

***Analysis By:*** Dennis Smith

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

***Position and Adoption Speed Justification:*** While the CMP market is continually changing, vendors and enterprise customers are getting a better feel about where such tooling can and cannot be used. Vendors are still being challenged with evolving customer requirements (for example, interfacing with multiple public clouds, cost transparency with workload optimization to remediate cost overruns and handling newer functions like containers and serverless deployments). At the same time, major market consolidation will continue. For example, many vendors, that initially targeted cost management, have been acquired as this functionality is becoming a part of the basic

CMP. Additionally many vendors in adjacent markets are acquiring CMP vendors and combining this functionality with asset management (software and hardware) and SaaS operational management. Cloud service providers (CSPs) and management service providers (MSPs) are also entering the market. Additionally, many long-standing vendors are introducing next-generation products, often targeting holes that their previous products had. Finally vendors in different markets (e.g., monitoring) are also entering the market. Some of the core CMP functionality is also being combined (for example, monitoring and analytics with cost management and resource optimization). The ability to serve both application developer and I&O personas is the key. This requires that CMPs be linked into the application development process without imposing a workflow that inhibits agility while also allowing infrastructure and operations (I&O) teams to enforce provisioning standards.

Organizations have an increasing need to address multicloud requirements. In some cases, they want to become internal cloud service brokers (CSBs) and manage public services that were previously acquired — often by lines of business (LOBs) outside the I&O organization — and have become difficult to manage operationally.

***User Advice:*** As CMP market volatility increases, IT organizations must:

- Consider CMP vendor's viability along with evaluating features.
- First consider native cloud services as an alternative or option versus CMPs, particularly if you favor depth with an individual cloud provider versus breadth across different cloud providers.
- Consider functionally focused tools (e.g., cloud expense management tool) if you only require a limited set of functionalities.
- Augment, swap out or integrate additional cloud management or traditional management tools for many requirements, because no vendor provides a complete cloud management solution.
- Standardize, because deriving value from your CMP will depend heavily on the degree of standardization offered by the infrastructure, software and services.
- Set realistic expectations on deployment times, as mature organizations implement CMP in a relatively short period (one to two years); however, less mature organizations may require two or more years to design effective, repeatable, and automatable standards and processes.
- Plan for new roles, such as cloud architects and cloud service brokers (CSBs), including developing skills in the financial management and capacity management areas.

***Business Impact:*** Enterprises will deploy CMPs (increasingly 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. Desirable IT outcomes include:

- Policy enforcement (e.g., on reusable standard infrastructure components).
- Reduced lock-in to public cloud providers, although at the cost of CMP vendor lock-in that can slow innovation.

- Enhanced ability to broker services from various cloud providers and to make informed business decisions on which 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.

***Benefit Rating:*** Low

***Market Penetration:*** 5% to 20% of target audience

***Maturity:*** Mature mainstream

***Sample Vendors:*** CloudBolt; Flexera; CloudSphere; Morpheus Data; Scalr; Snow Software; VMware

***Recommended Reading:*** "Magic Quadrant for Cloud Management Platforms"

"Critical Capabilities for Cloud Management Platforms"

## Continuous Configuration Automation

***Analysis By:*** Chris Saunderson

***Definition:*** Continuous configuration automation (CCA) tools enable infrastructure administrators and developers to automate the deployment and configuration of systems and software programmatically. They support the description of configuration states and settings, as well as the deployment of software binaries and configuration data. Most CCA tools have open-source heritage, with some offering commercial support. Commercial CCA tools have vendor support, role-based administration and more advanced management capabilities than open-source versions.

***Position and Adoption Speed Justification:*** CCA tools have proven critical to DevOps initiatives due to their ability to manage and deliver infrastructure and associated software and configuration changes as code. This enables inclusion of CCA-specified infrastructure as code into DevOps pipelines. CCA tools have continued to expand their reach into networking, containers, and into compliance and security roles. These tools are critical to DevOps initiatives, due to their:

- Programmatic access to infrastructure elements
- Ability to allow IT operations personnel to build an automation life cycle modeled on a software development life cycle
- Ease of experimentation, extensibility and access to active communities

- Potentially lower total cost of ownership (TCO) for significant configuration management capability

Enterprise adoption of these tools is hindered mainly by the IT skill sets needed to use them. Many I&O organizations lack individuals with basic scripting skills and source code repository management skills, let alone the skill to conceptualize and manage infrastructure as code. Developers and administrators may use them on a tribal basis, further inhibiting enterprisewide adoption. The growing use of containers has also created confusion about the role of CCA tools; however, Gartner believes that CCA tools and containers can be used in a highly complementary manner.

Organizations are increasingly using CCA tools for a broader set of deployment and automation functions beyond configuration management — for example, patching, application release orchestration, configuration auditing (e.g., for regulatory or internal policy compliance) and orchestration. As CCA tools are increasingly used in adjacent functions, organizations will experience the advantages of using these tools in new ways, but will also discover limitations relative to tools that are purpose-built for functions other than configuration management. An approach based on consistently applying a curated catalog of CCA tools will deliver effective productivity improvements to clients.

***User Advice:*** The overlap between infrastructure automation (IA) and CCA tools adds to the confusion around these tool markets. Clients should be clear about the role that CCA tools fulfill in their toolchain to ensure that duplication is minimized. Because CCA tools provide a programmatic framework, the costs associated with them extend beyond just the licensing cost (or the lack thereof), so enterprises should include professional services and training requirements into cost evaluations. In particular, most infrastructure and operations (I&O) organizations should expect to invest in training because not all infrastructure administrators have the skills needed to use these tools successfully. CCA tools have a learning curve, and it is tempting for developers and administrators to revert to known scripting methods to complete specific tasks. DevOps and IT operations leaders who want to maximize the value of CCA tool investments must ensure that their organizations' culture can embrace CCA tools strategically.

Use the following criteria to determine which CCA vendor and product is appropriate: internal IT skills, security and compliance capabilities, authentication and authorization support, alignment to other tools within operating environment, orchestration functionality, scalability, and platform support.

***Business Impact:*** By enabling infrastructure administrators and developers to automate the deployment and configuration of settings and software in a programmatic way, organizations across all verticals stand to realize:

- Agility improvements — By enabling continuous integration and delivery concepts to IT infrastructure management.
- Productivity gains — Via faster deployment and repeatable, version-controlled configuration of infrastructure.

- Cost reduction improvements — Via significant reductions in required manual interactions by highly skilled and high-cost staff by automating "day 2" operational tasks. Licensing cost reductions may also be achieved.
- Risk mitigation — Compliance improves via the consistent use of standardized, documented processes and configurations across physical and virtual infrastructures.

CCA tools can drive efficiencies in operational configuration management, as well as provide a flexible framework for managing the infrastructure of DevOps initiatives. They achieve this by integrating with other toolchain components — notably, infrastructure automation tools, continuous integration (CI) and application release orchestration in support of continuous delivery.

***Benefit Rating:*** High

***Market Penetration:*** 20% to 50% of target audience

***Maturity:*** Early mainstream

***Sample Vendors:*** Ansible; CFEngine; Chef; Inedo; Orca; Puppet; SaltStack

***Recommended Reading:*** "Market Guide for Continuous Configuration Automation Tools"

"Best Practices to Enable Continuous Delivery With Containers and DevOps"

"Use a Bimodal Approach to Improve the Selection of DevOps Continuous Configuration Automation Tools"

"Solution Path for Infrastructure Automation"

"Market Guide for Infrastructure Automation Tools"

## Entering the Plateau

### Cloud Migration

***Analysis By:*** Craig Lowery

***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 may be modernized through refactoring or rewriting, or potentially replaced with software as a service (SaaS) in the process.

***Position and Adoption Speed Justification:*** The process of cloud migration requires:

- Setting business objectives
- Determining what workloads can be moved to an external cloud service (or moved from one such service to another)

- Planning how to best migrate those workloads
- Executing the migration
- Learning to operate in the new cloud model

The tools to execute workload discovery and movement are mature. However, most organizations lack the expertise to plan and execute a migration. Migration service providers such as cloud infrastructure professional and managed service providers (MSPs, including global SIs) can provide other related services, in addition to the migration services. Migration service providers' experience and capabilities, such as the degree of modernization or transformation that can be applied to the migrated workloads, vary widely. Still, organizations often struggle with the new operational aspects of cloud computing, which can result in technically successful migrations that fail to meet business objectives.

***User Advice:*** Organizations can perform their own migrations or engage a service provider, usually an MSP. While customers sometimes migrate to SaaS without assistance, almost all successful large-scale migrations to cloud infrastructure and platform services (CIPS) are done in conjunction with a service provider. Most providers target hyperscale cloud service providers (CSPs), such as Amazon Web Services, Google Cloud Platform and Microsoft Azure. Migrated workloads use a mixture of the CSPs' IaaS and PaaS offerings. Experienced providers can help IT leaders think through their objectives and determine what the end state looks like from a technical and organizational perspective. Fully capable providers have a well-structured "migration factory" process, strong project management and the technical staff to deliver timely implementation.

I&O leaders electing to perform their own migration should consider purchasing cloud migration tools or using the CSP's native migration tools. When using a migration service provider, I&O leaders must clearly define their use cases and understand that provider strengths will vary. I&O leaders should also consider the compatibility between the provider's tools and processes, and their own tools and processes.

Application leaders should also consider what approach is best for modernizing an existing application. Although rehosting without modification might be easiest, it brings far fewer benefits than replatforming, refactoring, rebuilding or replacing the application. The market consensus is that rehosting ("lift-and-shift") migrations consistently fail to meet expectations, with cost and security issues being most common. Although some rehosting migrations are still done for expediency, customer expectations of cloud-native benefits have become mainstream.

***Business Impact:*** Most organizations desire to move most or all their workloads from their own data centers into the public cloud, but a complete removal to public cloud is rare for large enterprises. SaaS opportunities aside, the fact that rehosting is not as effective as first thought — combined with the investment required to properly analyze, migrate, and transform applications — leads many organizations to delay a cloud-only strategy. Most organizations will realistically be in a hybrid IT configuration indefinitely, with an ever-shrinking set of applications both on-premises or in colocation facilities, and a growing application set in the public cloud. Single-application migration can be accomplished in a matter of days or weeks. Additionally, if application transformation is de-emphasized, organizations can move most of their workloads to public cloud within a year.

However, only organizations that adopt high degrees of standardization, cloud-native capability and organizational change management will maximize all cloud benefits.

***Benefit Rating:*** Moderate

***Market Penetration:*** 20% to 50% of target audience

***Maturity:*** Mature mainstream

***Sample Vendors:*** Accenture; Bespin Global; Capgemini; Cognizant; Deloitte; Logicworks; Rackspace; Smartronix; Tata Consultancy Services; Wipro

***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 Migration Impact Calculator"

"Cloud Cost Scenario Planning Tool"

"Ignition Guide to Creating a Migration Plan for Public Cloud"

## DevOps

***Analysis By:*** George Spafford; Joachim Herschmann

***Definition:*** DevOps is a customer-value-driven approach to deliver solutions using agile methods, collaboration and automation. DevOps emphasizes people and culture to improve collaboration between development, operations and other stakeholders to navigate uncertainty, and accelerate the delivery of customer value. DevOps implementations use architecture and tools to improve the flow of work.

***Position and Adoption Speed Justification:*** DevOps doesn't have a concrete set of mandates or standards, or a known framework (such as ITIL); thus, it is subject to a more liberal interpretation. In general, it is about cross-functional teams collaborating to deliver business value faster. DevOps is associated with processes, tools and organizational styles intended to optimize the flow of work across the application life cycle, from development to production. DevOps concepts have become widely adopted for initiatives with a style of work that is focused on exploration and agility, including digital business, machine learning, mobile apps, IoT. Also, there is potential for use in more traditional enterprise environments; however, every implementation is unique. Good practices are emerging, the sharing of lessons learned is vibrant among practitioners. Vendors are developing and delivering supporting tools and professional services. While some new adopters are having challenges clients report that DevOps does deliver value.

***User Advice:*** DevOps initiatives must be iterative, focused on business value and have executive sponsorship, with the understanding that new team(s) will have to make an often-difficult organizational philosophy shift toward the development of agile capabilities. DevOps hype remains

elevated among tool and service vendors, with the term applied aggressively and claims outrunning demonstrated capabilities. Many tool vendors are adapting their portfolios and branding their offerings as DevOps-related to gain attention. Some vendors are acquiring smaller point solutions specifically developed for DevOps to boost their portfolios. Clients are recommended to clearly tie investments to business outcomes to help improve internal adoption.

IT organizations must establish key criteria that will differentiate DevOps tooling traits (strong toolchain integration, workflow, automation, etc.) from traditional management tools. Both development and operations should look to tools to replace custom scripting with improving deployment success and cycle times through more predictable configurations and seek to continually improve the flow of work via refactoring.

IT organizations should approach DevOps as a set of flexible guiding principles. Start small and focused — don't try a "big bang" approach. Select a product that is politically friendly, and offers acceptable value and risk involving development, operations and other critical stakeholders, such as information security and architecture. Stakeholders need to work together to accomplish the business objective, while learning how to organize and determining what methods and tools to use. At a minimum, seek to continually improve the flow of work from developer through to the new or changed application being in production and the customer receiving the promised value. These stakeholders must also collaborate to scale efforts.

***Business Impact:*** DevOps is focused on delivering customer value and enables hypothesis-driven development and the aggregation of data to make decisions about future functionality. Release cadence can be varied to meet demands for organizational learning and change absorption. DevOps approaches are made possible by the adoption of continuous learning, improvement and incremental release principles adopted from agile methodologies. Smaller, more frequent updates to production can work to improve organizational learning and overall quality, including both stability and control, thus reducing risk. A successful DevOps implementation will improve the delivery of customer value. This delivery of value justifies the scaling and expansion of DevOps using an iterative approach.

***Benefit Rating:*** Transformational

***Market Penetration:*** More than 50% of target audience

***Maturity:*** Mature mainstream

***Recommended Reading:*** "Adopt an Iterative Approach to Drive DevOps Success in Large Organizations"

"DevOps — Eight Simple Steps to Get It Right"

"DevOps Primer for 2019"

"Three Ways Midsize Enterprises Can Maximize Value From DevOps"

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

"DevOps Success Requires Shift-Right Testing in Production"

"Avoid Failure by Developing a Toolchain That Enables DevOps"

"Top 5 Causes of DevOps Failure and How to Avoid Them"

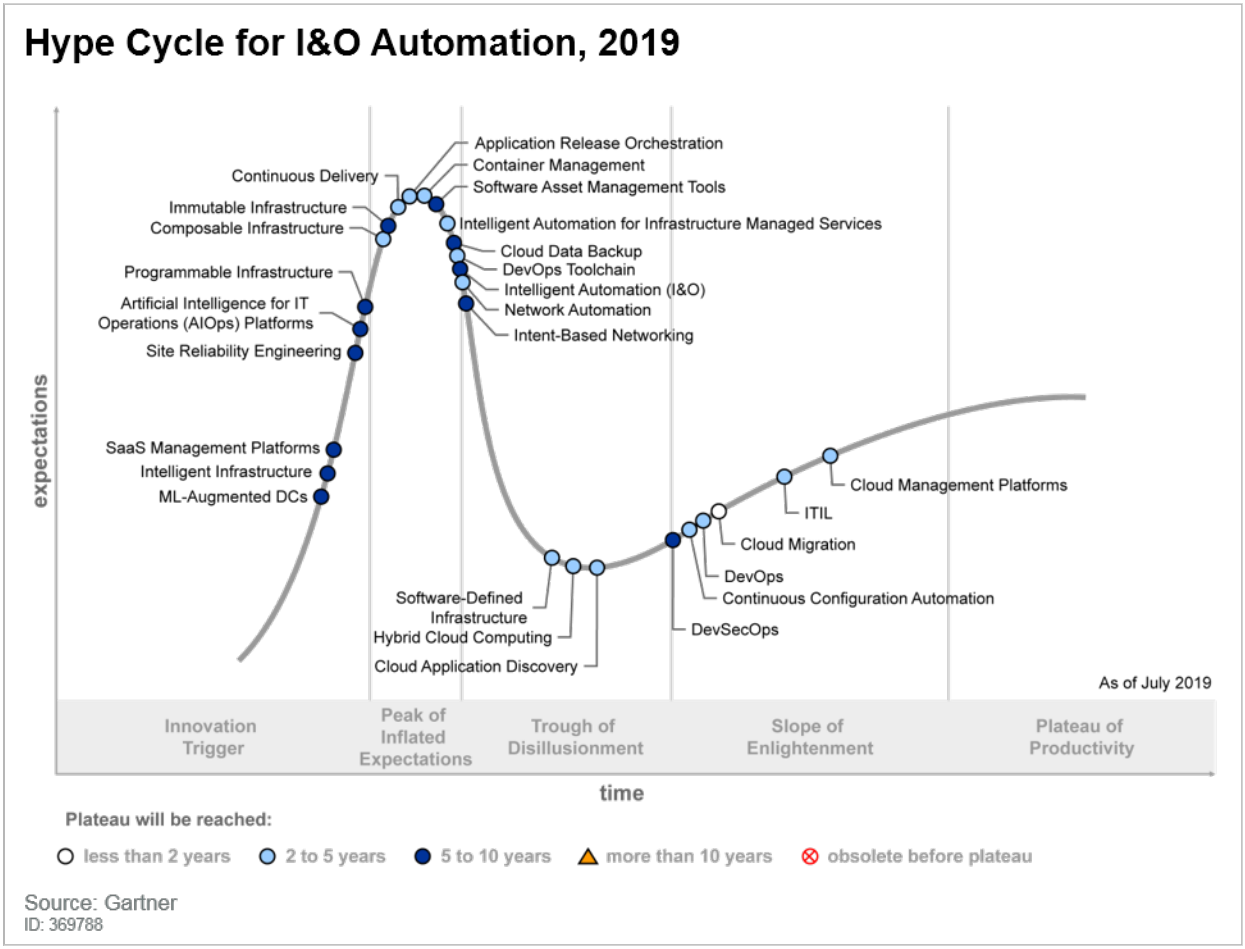
"How to Avoid Compliance and Audit Concerns When Using DevOps"

"How to Scale DevOps by Building Platform Teams"

"Top SRE Practices Needed by Teams Scaling DevOps"

## Appendixes

Figure 3. Hype Cycle for I&O Automation, 2019




Source: Gartner
ID: 369788

## Hype Cycle Phases, Benefit Ratings and Maturity Levels

### Table 1. Hype Cycle Phases

| Phase | Definition |
|---|---|
| *Innovation Trigger* | A breakthrough, public demonstration, product launch or other event generates significant press 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 technology is pushed to its limits. The only enterprises making money are conference organizers and magazine publishers. |
| *Trough of Disillusionment* | Because the technology 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 technology'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 technology 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 technology to reach the Plateau of Productivity. |

Source: Gartner (August 2020)

### Table 2. 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 (August 2020)

Table 3. Maturity Levels

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

Source: Gartner (August 2020)

## Gartner Recommended Reading

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

Understanding Gartner's Hype Cycles

Leadership Vision for 2020: Infrastructure and Operations Leader

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

Top 10 Trends Impacting Infrastructure and Operations for 2020

Hybrid Digital Infrastructure Management: A View From the Top

Data Center Infrastructure Primer for 2020

15 Infrastructure KPIs for Digital Business Transformation

Magic Quadrant for Cloud Management Platforms

**GARTNER HEADQUARTERS**

**Corporate Headquarters**
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

**Regional Headquarters**
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp