ScienceLogic

# Unlock the Power of AIOps: From Vision to Reality

# Unlock the Power of AIOps: From Vision to Reality

## CONTENTS





ScienceLogic

# The Promise of AIOps

For businesses across the globe, the word "agility" has evolved to become more than just a buzzword. It signifies a customer expectation that businesses will be nimble and possess the foresight to anticipate and meet their needs. For enterprises, in return, the necessity to be agile has served as a catalyst for new initiatives and technology deployments, allowing them to rapidly adopt the 'fail-fast' model for innovation and devise ways to enhance customer's digital experiences.

The quest for business agility has led to today's era of digital transformation where organizations are employing new operational strategies that prioritize speed, precision, and rely on new, highly-ephemeral technology to make it all happen.

However, the rush to adopt new components has its consequences – particularly around their management.

Applications are increasingly constructed under a DevOps model that adopts multiple microservices – transient services or auto-scaling instances that may only appear for a few seconds before going dormant. Beyond the applications, their underlying infrastructure, once relatively fixed and physical, is now virtualized, complex, and capable of changing in microseconds.

The new dynamic of having virtualized technology spin up or down as needed represents a sea change compared to five years ago and presents considerable challenges since traditional IT management tools and associated manual processes cannot keep pace. Likewise, prior operating procedures that used manual processes or simple rules-based policies are rapidly becoming outdated and unworkable, as human labor cannot react quickly enough to maintain services to customers.

**A new operating model is required, which moves at machine speed. Successful execution hinges on mastering the ephemeral IT landscape where CIOs are struggling to answer critical operational questions such as:**

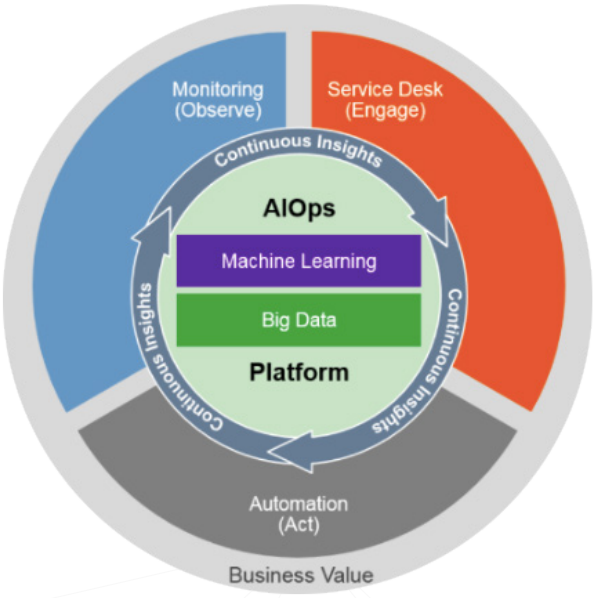
- *Where to place workloads for optimal performance and cost?*
- *How to connect apps to infrastructure to maximize availability and attain service health views?*
- *How to provide ongoing support in a dynamic, digital world?*
- *How to reach optimal levels of agility?*

To achieve the agility necessary for digital transformation and customer expectations, CIOs need to forgo yesterday's manual processes and harness the power of artificial intelligence (AI) and machine learning (ML) tools to help them automate.

An entirely new approach is needed, which is the promise of AIOps.

# The Evolving State of AIOps

Artificial Intelligence for IT Operations (AIOps) is traditionally defined as the combination of big data and machine learning. However, based on the increasing complexity and dynamic nature of the IT landscape (and to really achieve the benefits of AIOps and make the operational data actionable), the current definition needs to be refined. Specifically, big data is too broad and typically encompasses data that's unwieldy, unactionable, and unorganized. To truly achieve the benefit of AIOps, more emphasis needs to go into the quality of the operational data.




(Graphic courtesy of Gartner)

**While big data implies data quantity, it is the quality of the operational data being collected that holds the key to successful automation with AIOps.**

Successful AIOps hinges on two important aspects of data quality.

- **First, the data must be up to date.**
  Timeliness is even more critical with the advent of containerized services that are highly dynamic and short-lived. Traditional monitoring systems might update their asset base every 15 minutes via an SNMP polling cycle, which is marginal for virtualized or cloud devices, but too slow for containers, microservices and serverless compute. Similarly, service management systems typically update their CMDB only daily or weekly. As a result, they're highly ineffective since the infrastructure has 'moved on' by the time the data is used. To be effective and make accurate decisions in the current environment, IT operations (IT Ops) teams need real-time data.

- **Second, the data must have context.**
  Context makes the operational data actionable. A recent study by Digital Enterprise Journal found that more than 70% of the operational data collected by IT organizations is not considered actionable[1]. In the current IT environment, operations teams have never had access to so much data, but because the data lacks context, they are unable to act upon it effectively. By applying context – a knowledge of the relationships and associations between IT elements and their logical and physical neighbors, decisions can be taken that

1 http://dej.io/17-areas-shaping-it-operations/

address root causes rather than symptoms, and ensure those relationships are preserved during automation or remediation steps. At its core, context shows relationships, such as the relationship between a virtual machine and its associated storage, or between an application and its underlying compute, OS, storage and network components.

For AIOps to succeed, real-time data - delivered with context - is a mandatory requirement and will be the only sound basis for advanced automation and machine learning to be successfully adopted in the enterprise.

## The Importance of Context

Context is critical because it brings additional insight by adding meta-data related to device or service metrics. This meta-data may be simple asset records or more importantly a set of relationships, connections or associations between a device or service and other related devices or services.

**Context can take multiple forms and informs IT Ops of error conditions, such as:**

- ***Which production services are impacted and how important are they to my business?***
- ***Did these events happen at the same time?***
- ***Is there a dependency? How many other items are related?***
- ***What change preceded this event?***

### Infrastructure Mapping

Infrastructure mapping is essential for successful AIOps. Understanding which infrastructure elements are deployed as well as where they are deployed and their logical and physical dependencies, provides critical insight into the interactions between applications and their underlying infrastructure. For example, the attachment of storage units to virtual machines may be monitored by both a storage tool and a virtualization manager. Without infrastructure mapping, the storage tool could be unaware of VM associations, and the virtualization manager will have no view of related storage. Infrastructure mapping offers a complete picture, providing the relationship between each component. When an application is degraded due to a slow connection between a VM and its storage, neither point tool will show a problem.

Similarly, a lack of context can lead to incorrect prioritization of problems. By adding context such as associated dependencies and connections, we can determine whether a failed device is an essential component of a mission-critical business service, or if a routine follow-up will suffice.

### Application Mapping

A full understanding of an application's topology and its relationship to the underlying infrastructure are key aspects of AIOps. Since AIOps addresses the holistic IT landscape – and not just applications or the infrastructure – application mapping is important to the data enrichment process. By mapping the topology of an application to its underlying infrastructure, IT Ops can see the physical and/or logical relationships between elements. Application mapping is also used to specifically identify malfunctioning items within the business service and can be used to trace the business-level impact of fault conditions. Application topology will come from many different sources. No single source will have maps for all applications, so a complete picture may be fused together from several disparate sources, including APM, NPM, Orchestration, etc.

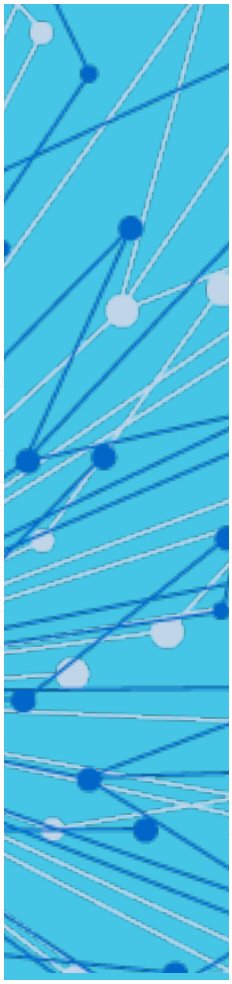
### Business Service Mapping

A mission-critical business service - like an e-commerce site - may include hundreds of smaller services (credit card validation, order placement, shopping cart, account profiles, etc.) and comprise thousands of devices. In such cases, it's important to enable executive oversight with views of service health, availability and risk, rather than rely on arcane views of specific server or network device metrics that become meaningless and obfuscate the real picture of service performance.

The ability to map out the components of mission-critical business services and track them – in real time as a group, enables IT Ops to prioritize their efforts on maintaining and supporting the services that affect the bottom line and customer satisfaction. Where possible, a predictive view enables operations teams to forecast future capacity bottlenecks or performance issues and ensure the availability of critical business services is not compromised.

## Real-World Problems that AIOps Addresses

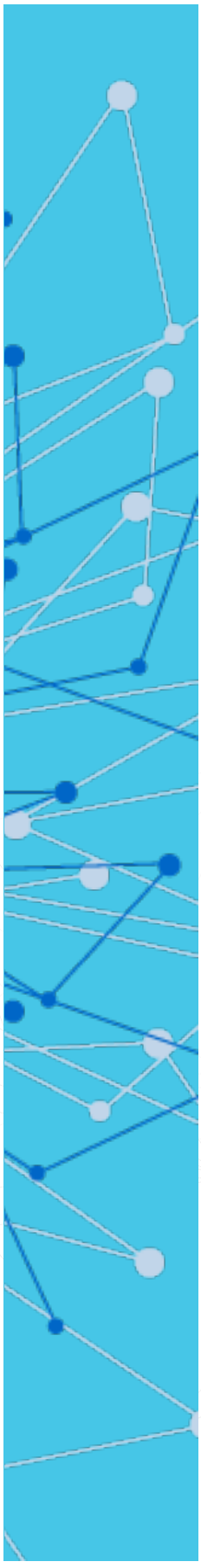
As a result of careful data preparation, enrichment, and the application of context to operational data, an AIOps approach can now address several major operational challenges in the enterprise that are difficult to solve with traditional tools and manual methods. Below are some real-world problems that AIOps is already being used to address:



### Identify Business Service Impact

The ability to view IT at the business services level rather than at the infrastructure level helps IT executives, their business unit colleagues, and customers manage the performance of critical business services with greater clarity. Traditional IT monitoring platform tools have long been capable of this analysis but required extensive professional services to create and update static service models – a very costly and unwieldy approach. Modern AIOps platforms, by contrast, can collect data and apply business context and topology meta-data to construct service maps that enable the tracking of entire business services in real-time.  This results in an understanding of the impact of any potential failures on the business, and a holistic service view instead of component-centric views.

Given topological or organizational context, an AIOps platform can bring business service mapping and real-time insight to the executive level without clouding their view with superfluous infrastructure detail. By providing real-time views of high-level service parameters (i.e., health, availability and risk) without technical knowledge of the underlying server, storage or network conditions, non-technical users can rapidly gain service visibility. In particular, the risk associated with a given business service is a factor that can be calculated directly from an understanding of topology. However, this is not well suited to typical AI/ML techniques. For example, while a vast amount of historical data may show normal ranges of behavior and connectedness of events, AI/ML without topological awareness will not generate a critical risk event because a lack of redundancy may leave an application just one failure away from an outage.



## Expand the Reach of Traditional APM Systems

Rapid fault isolation and mean time to repair (MTTR) reduction have always been important. However, in today's ephemeral environment, they're also more difficult to achieve. With highly fragmented applications running across ultra-dynamic and hybrid infrastructures, traditional APM systems, troubleshooting tools and manual triage methods are rendered obsolete.

By leveraging the continuous discovery of data that's accurate, captured in real-time and possesses context (due to advanced application mapping and application-to-infrastructure mapping in real time), IT Ops can rapidly triage complex application performance problems down to their related underlying infrastructure issues – even for packaged applications where code-based instrumentation is not possible. Without contextualized data, mapping applications to their underlying infrastructure is either cost prohibitive or impossible, resulting in more application outages and severely impacting business productivity, cost, and customer satisfaction.

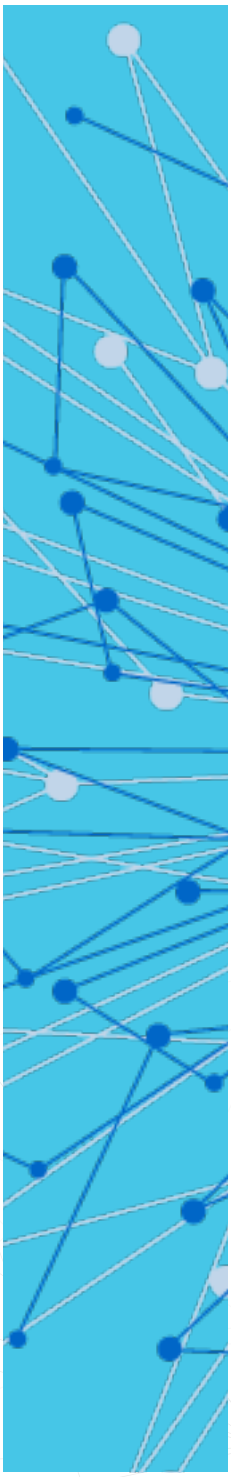
In some cases, the addition of a machine learning engine that's trained by clean, contextualized data from an AIOps platform can bring added business impact analysis that helps prioritize which problems have the most effect on business performance – perhaps by applying business process knowledge such as supply chain characteristics. Training a machine learning engine with clean, contextual data avoids having the ML engine return false positive results or taking too long to respond.

A substantial reduction in event noise through data reduction and enrichment can also lead to significantly reduced incident volume, enabling operations teams to focus on solving the right problems and avoid chasing false positives. The flow of clean incident data to service management systems leads to major cost savings, outage reduction, and staff productivity improvements. Ultimately, the main benefit is a substantial reduction in application downtime, either by heading off problems proactively or through more effective triage of problems when application performance is degraded but the application is still functioning.

## Automating Incidents with an Enriched CMDB

As the need for agility at the enterprise level increases, IT must also become agile. The only way to achieve the necessary level of agility in today's environment is with automation, such that IT can adequately respond to rapidly changing business needs with minimal disruption or compromise in service quality.

To function effectively and accurately, an AIOps engine or automation platform needs access to clean data such that automation decisions are accurate, and no false positives ensue. Automation in this context implies a significant degree of self-healing and automated remediation, which can only be accurate if based on clean underlying data sets. Automations can include automated incident generation, incident handling, automated triage, notifications, auto-remediation (such as server or VM re-boot or autoscaling), and other automated functions.
To make service delivery more agile, one of the key pressure points to address is



the configuration management database (CMDB). Unfortunately viewed as the weakest link in the chain, even the most modern CMDBs are typically found to be inaccurate and/or out of date. While applications and infrastructures are increasingly dynamic, the CMDB often remains static. By enriching the CMDB with timely, accurate, contextualized data, IT Ops can now use the power of a CMDB as a basis for effective automation. As an example, an enriched CMDB can power a fully automated incident handling process by routing incidents to the right operations teams for investigation while eliminating false positive incidents and enriching the incident with contextual metadata, relationships and diagnostic detail that help reduce trouble resolution time.

As a result of automating the incident handling process, organizations can reduce the cycle time for incident processing, save on staffing for incident handling, avoid false positives and the mis-routing of incidents, and establish an accurate CMDB--which can serve as a future 'single source of truth' for effective automation across the enterprise.

## Taming Cloud Sprawl

Many IT operations organizations lack adequate visibility and control over their cloud instances – especially those deployed in a public cloud service. As a result, they have limited visibility into under-used or over-used resources or of unusual or unauthorized activity associated with their account. These factors add to the risk that unchecked cloud spend can quickly morph into cloud sprawl and leave organizations with expensive unintended consequences. The spiraling cost of cloud services can inhibit broader cloud deployment as organizations rein in their cloud spend and forgo some of the other benefits that cloud services bring.

By adding cloud performance, configuration and log data, IT operations teams can establish policies to determine appropriate levels of authorization and proactively identify when and where excessive levels of compute are employed. Cloud data may include records of cloud compute instances that were started, stopped, rebooted or terminated, as well as total instances running over a period of time.

Having collected this data, an AIOps platform can use it to notify users or administrators of policy violations, automatically create an incident, or even automatically shut off unauthorized access, unauthorized instance types, or excessive usage levels by a given user. The major business benefits are cloud cost containment, staff savings and enhanced security.

# Conclusion

We have discussed the major challenges that AIOps can address for enterprise CIOs faced with navigating their companies through large-scale digital transformation. The pressures induced by the drive to become more agile – and the consequential changes to the IT landscape – are impossible to solve with manual labor since humans cannot react quickly enough. Only by the wholesale adoption of automation, embodied in an AIOps approach, can the CIO achieve true agility within IT. But for AIOps to succeed, the operational data it feeds on must be clean and contextualized. The world's most advanced neural-nets are only as good as their training data.

Collecting and preparing clean and contextualized operational data is the subject of our companion paper, *Unlock the Power of AIOps: It's All about the Data*. In the paper, we describe the essential steps to take in successfully deploying an AIOps platform.