

# AIOPS

# MANIFESTO

The Role of AI in Assuring Digital Transformation

## Authors

Will Cappelli  
Clive Longbottom  
James Governor

May 2019

# Table of Contents

<b>Executive Summary</b>	<b>3</b>
<b>The Need for AIOps</b>	<b>4</b>
<i>Figure 1 - The IT Operations Management Cycle</i>	5
<b>The History of AI</b>	<b>6</b>
<i>Figure 2 - The History of AI</i>	6
<b>The Five Dimensions of AIOps</b>	<b>7</b>
Data Set Selection	7
<i>Figure 3 - The Five Dimensions of AIOps</i>	8
Pattern Discovery	9
Inference	11
Communications	12
Automation	13
<b>The Market Context for AIOps</b>	<b>14</b>
Log Management & Data Aggregation	14
Unified Monitoring	14
<i>Figure 4 - Adjacent Markets</i>	15
Event Correlation	16
Topology-based Analytics	17
Service Management	17
Smart Alerting	18
<b>The Challenges of Digital Transformation</b>	<b>19</b>
Separation of IT Systems from Business Processes	19
IT's Big Data Problem	20
Fluid & Ephemeral Infrastructure	21
<b>The Failure of Traditional ITOM Technologies</b>	<b>22</b>
<b>How an AIOps Platform Solves These Challenges</b>	<b>23</b>
<i>Figure 5 - The AIOps Workflow</i>	24
<b>The Bottom Line</b>	<b>26</b>
<b>About the Authors</b>	<b>27</b>
<b>About AIOps Exchange</b>	<b>27</b>

# Executive Summary

The past decade has seen a fundamental transition in the way that businesses and the economy as a whole operates. IT, once largely concentrated on record keeping and the facilitation of back office processes, has now become the primary domain within which almost all business processes – from production through trade to consumption – are realized. Its centrality has radically altered IT itself. The digitalization of business is predicated on IT's enablement of rapid adaptability to changing market needs. This has forced developers of IT systems to switch from monolithic to modular designs, centralized to distributed architectures, static to dynamic configurations, and multi-year to ephemeral life-spans at the component level.

## FEEDBACK ON THIS PAPER?

Submit your comments to the authors at  
[INFO@AIOPS-EXCHANGE.ORG](mailto:INFO@AIOPS-EXCHANGE.ORG)

# The Need for AIOps

WHILE SUCCESSFULLY SUPPORTING digital transformation, the revolution in IT systems has wrought a new set of challenges for IT Operations. It has become absolutely critical that IT Ops deliver high-quality services continuously and consistently. Unfortunately, because today's systems are modular, distributed, dynamic, and ephemeral, the opportunity for outages and other service interruptions has multiplied. The IT Operations Management (ITOM) function is charged with monitoring system performance. Incident management processes include the analysis and detection of system issues, intervention when needed to address any issue, and timely and effective resolution. The strategic significance of IT Operations has only grown given IT's newfound centrality in the face of the staggering scale and complexity of modern environments in their charge.

There are four properties that make IT systems more flexible and adaptable, but also more problem-prone and far more difficult to observe, analyze, and modify:

1. The amount of data that IT Ops teams need to analyze has exploded with the multiplication of components and the dynamic nature of their interconnections.
2. The messages and event records of observed system data are riddled with noise and error, since components are distributed and autonomous.
3. The root cause of performance problems is almost impossible to determine, given the ephemerality and complexity of component interactions, even when aided by visual analytic tools.

**AIOPS SOFTWARE MARKET**

**\$2.5B IN 2018**

*25% Annual Growth Rate*

## THE IT OPERATIONS MANAGEMENT CYCLE



4. The speed with which system states change require that plans be made and interventions accomplished in real time, preferably in minutes and seconds.

The burdens of modern IT Operations Management can be ameliorated, even largely removed, using Artificial Intelligence (AI). The market for AI applied to IT

Operations, or “AIOps” for short, is growing in parallel with digital transformation. AI has emerged as the key to mastering both the explosion in system data and the automation of human-to-machine interactions.

Unfortunately, the term ‘AI’ is ill-defined and often misunderstood.

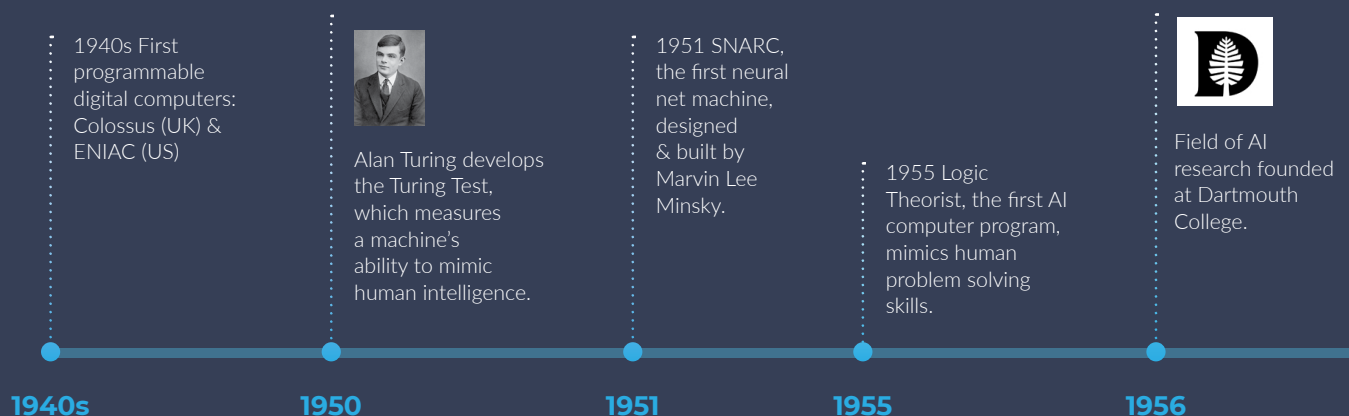
# The History of AI

AN EXAMINATION OF the history of AI (see *timeline*) reveals an industry plagued by fits and starts. Frankly, the jury is still out on whether its promise will be fulfilled for business in general. We humans, for all of our predictability, are still capable of genuinely novel responses to the situations in which we find ourselves. Human qualities like common sense and intuition stymie the ability of even very sophisticated learning algorithms to build robust models.

However, a strong case can be made that when it comes to IT systems management, the limits on the overall applicability of AI are not a factor. Modern IT systems are undoubtedly complex. Indeed, the patterns that govern their behavior exceed the

observational and analytical abilities of even the most skilled human operator. Yet at their root are components that work in very finite, describable ways and are subject to a set of finite, describable human actions. Despite the booming, buzzing confusion and genuine complexity of today's digital business, there is no genuine novelty in the practice of IT support. Without having to confront novelty, AI's application of statistical pattern discovery has a good chance of succeeding. This explains why, over the span of AI's sorted history, the ITOM software market was one of the few sectors of the economy where rules-based, logic-driven AI delivered actual value.

## THE HISTORY OF AI IN IT OPERATIONS



# The Five Dimensions of AIOps

WE HAVE IDENTIFIED five distinct types of algorithm that constitute the brain's cognitive processes. In order to satisfy the requirements of ITOM, all five must be brought into play. The good news is that current computer economics make feasible the simultaneous deployment of all five dimensions. Let's discuss them in the sequence that the human brain follows in discovering, analyzing, and dealing with a problem. Many AIOps platforms are structured to facilitate a similar sequencing of algorithmic applications. Where they are lacking, human intervention is expected to fulfill the role.

## ► DATA SET SELECTION

The AIOps platform, like human decision making, is first faced with a continually shape shifting influx of data. These data items indicate a vast array of objects, events, and trends in the environment clamoring for attention. They are not all of equal significance. A human being, like an IT Ops team, has limited resources so some kind of selection and prioritization of problems must take place. For example, AIOps picks up data about a poorly performing application in the Sao Paulo data center, a poorly performing database in London, and a network outage on the link that connects Singapore to Mumbai. If the organization only has resources to cope with two issues at any given time, then economics and policy must

1958 "Reasoning as search" algorithm applied in programs like General Problem Solver.

DARPA doles out \$M research grants to MIT, Carnegie Mellon & Stanford.

AI lab at Edinburgh University founded in the UK.

**\$M**

Natural language processing debuts in programs like STUDENT & ELIZA.



HAL 9000 stars in the movie 2001: A Space Odyssey

A robot arm learns to stack blocks, the first micro-worlds driven program.

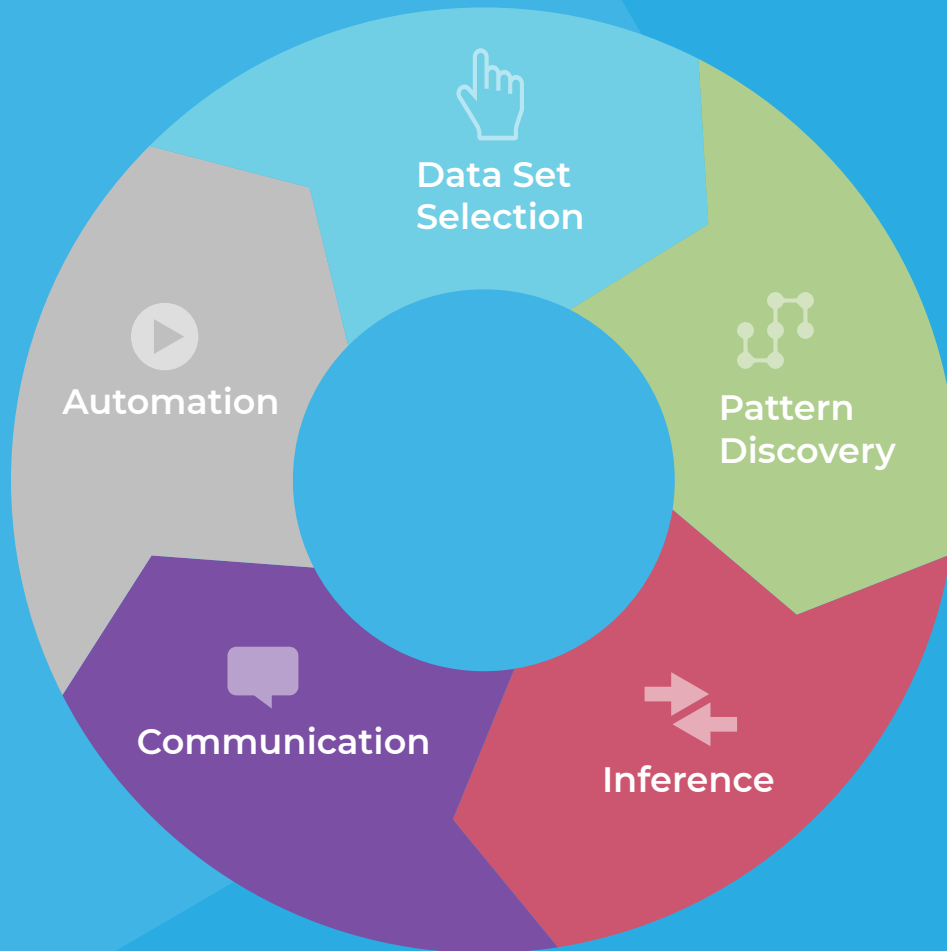
1958

1963

1964

1968

# THE FIVE DIMENSIONS OF AIOPS



## THE HISTORY OF AI IN IT OPERATIONS

"AI Winter" begins, when overly optimistic predictions fail to materialize.

Research funding dries up after the harshly critical Lighthill Report.

1973

### Prolog

The successful logic programming language Prolog introduces rule-based decision making.

1970s

Japan invests billions into AI with Fifth Generation Computer Systems initiative.

UK and US respond with Alvey & MCC projects.

Expert Systems debut, using logical rules based on expert knowledge for decision making.

Knowledge engineering becomes the focus of mainstream AI research.

1980

Expert Systems market grows to \$1B annually as corporations adopt commercial hardware & software solutions.

**\$1B**

1985



dictate some kind of prioritization. This is data set selection.

There is a more fundamental issue, however. A large percentage of the data initially encountered by the AIOps platform does not provide any new information about the state of the environment. Recall that much of the data items being generated by any IT system is either redundant or corrupt. To control both time and cost, these data items must be eliminated before any further analysis is carried out. Data set selection algorithms must be deployed to clear away the debris and clear the way for sound analysis.

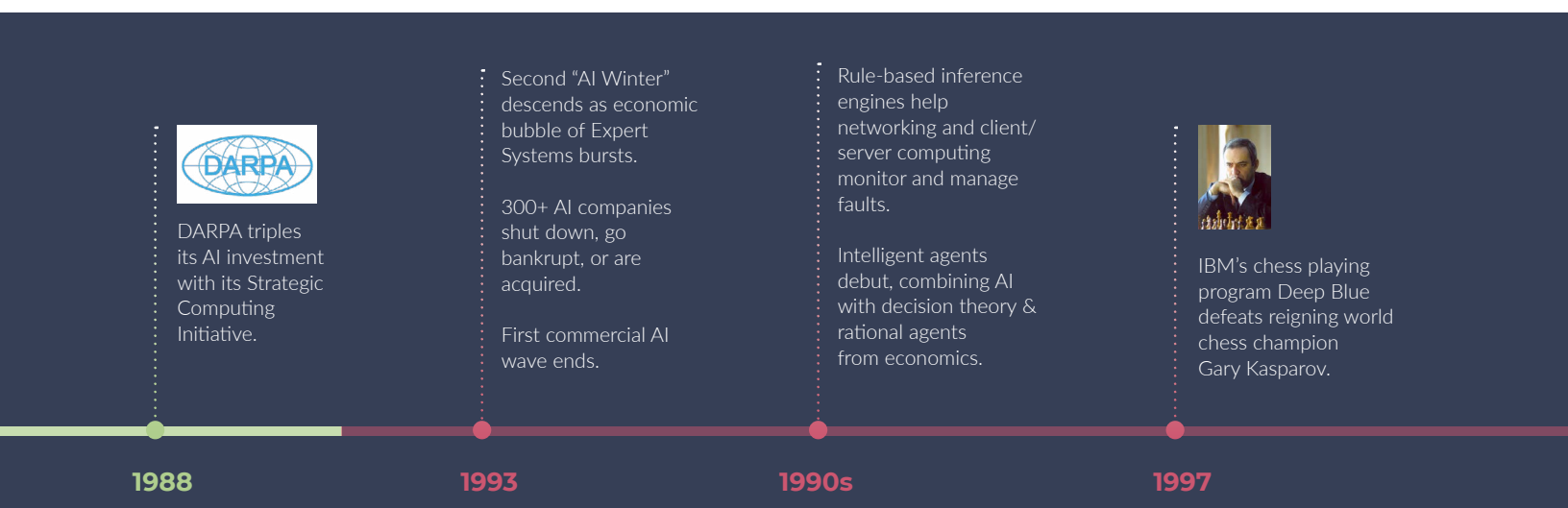
There are very few commercial implementations of this sort of algorithm. Why? First is the fact that such algorithms typically require the invocation of relatively obscure mathematics. Second is the fact that many regard data set selection as a sub species of pattern discovery and hence, fail

to see the need for it. Finally, and perhaps most importantly, most AIOps vendors and practitioners do not recognize the severity of the noise and redundancy problem in their data sets to begin with.

▶ **PATTERN DISCOVERY**

Once the appropriate data sets have been selected and the debris of noise and redundancy cleared away, the next dimension of algorithm comes into play. Algorithms in this dimension survey the data items contained within those data sets and, through various means, attempt to discover patterns governing that data. These patterns can take a number of forms (*See the table on page 11.*)

As simplistic as such a template extraction and matching algorithm might appear, it is in fact the master pattern discovery paradigm for many systems in the AIOps market, particularly technology based on rules and



logic. This approach to pattern discovery does not discover anything new about the data. Instead, it looks carefully and calls out what is already there.

There are, by contrast, other approaches to pattern discovery that analyze features of the data items to determine whether or not a mathematical equation (either deterministic or statistical) would be capable of describing the set. These approaches actually add new information beyond what is contained in the data set itself. Since the patterns proposed by these algorithms go beyond the content of the data set, their applicability is not certain but instead based on probabilities. Because they actually expand what is known about the data, they often deliver richer, more actionable results than template extraction.

Commercial application of pattern discovery technologies has been at the heart of business excitement about AI over the last five years. Be aware that there are three distinctions between applications of this algorithm type.

**Supervised versus Unsupervised.** This is a distinction between the mathematical approach to pattern discovery. In a supervised approach, the algorithm takes as input not only the data set itself but also a set of data classifications which are fed to it. The data is partially labeled and that labeling becomes crucial to the algorithm's function. In an unsupervised approach, the algorithm works directly on the data itself. No preparation or labeling of data is required.

## THE HISTORY OF AI IN IT OPERATIONS

The term "AI" goes out of vogue, replaced by descriptors like informatics & cognitive systems.

Event management systems emerge combining inference rules with routing & notification capabilities.

2000s

### IBM Watson®

IBM's Watson, defeats the two greatest human champions of TV game show *Jeopardy!*

2011

AI expands into new research areas like deep learning neural networks and "strong AI"

Driven by the Big Data problem, use of AI expands across industries.

Statistical pattern discovery algorithms re-emerge to automate the analysis of large data sets.

2010s

### Gartner

The total AI market grows to \$8B+

Gartner Research coins the term "AIOps" as the evolution of the IT Operational Analysis market.

2016

Data Set	Pattern 1	Pattern 2	Pattern 3
1. John runs to the store. 2. Mary runs to the store. 3. James runs to the library.	“___runs to the store.” <i>Items 1 and 2</i>	“___runs to the library.” <i>Item 3</i>	“___runs to the___.” <i>All items</i>

**Training Requirement.** Another important distinction is the degree to which the algorithm requires a training period in order to determine which pattern actually governs the data set in question. With many popular pattern discovery algorithms (e.g. single or multi-layered neural networks), the data set is fed piecemeal to the algorithm and gradually settles on a pattern over time. Other approaches allow for instantaneous or nearly instantaneous pattern discovery.

**Tracing.** The final distinction is whether or not it is possible to trace how the algorithm concluded that the specific pattern presented is the one that governs the data set. Unfortunately, it is not always possible to follow and justify the steps that algorithms take. This is a problem of the math itself, not a lack of human comprehension. There is often no mathematical or logical reason that can be cited for the algorithm’s success. In contrast, other approaches (e.g. Support Vector Machines) achieve successes that

can be explained with mathematics, even if the calculations and concepts are deep and complex.

What is the point of pattern discovery? Once the noise and redundancy has been eliminated, what is left over is data pointing to events that are taking place in the IT environment. These priorities need to be observed, analyzed, and manipulated. It is more important to know how two events — such as a router failing and latency in an application — are related to one another. Do these events occur close to one another in time or space? Could they be different manifestations of the same problem? Can these events be clustered together in one way or another? Patterns link events together in various ways to then allow correlated clusters to be created.

## ► INFERENCE

Once patterns have been discovered, their full implications need to be drawn out. Inference algorithms can take a number

of forms. Statistical patterns require classic statistical inference techniques. If the patterns are expressed as declarative sentences, then logic can be used.

A very important subclass of inference algorithms apply causality. A pattern, for all the richness of information it provides, ultimately tells us what is actually the case. Understanding the underlying cause of any given event requires some deductive reasoning. Inference algorithms have the ability to perform “what if” experiments on the data sets described by the pattern. For example, we may know that a particular level of CPU usage causes user response time to lengthen. Inferential techniques allow practitioners to reason out the consequences and establish a causal link among different events.

During the 1980s, inferential algorithms received commercial attention in the form of “expert systems”. These were nothing more than embodiments of very simple inference algorithms. But because they lacked any kind of automated pattern discovery capability, the premises of the inferences executed by the algorithms had to be manually fed to them. Back then this was known as “knowledge engineering”. Today’s rules-based AIOps platforms combine the basic template extraction approach to pattern discovery with simple inference techniques.

#### ► COMMUNICATIONS

Once the inferences are made and the conclusions about the significance of the discovered patterns drawn, these conclusions need to be communicated. This fourth algorithmic dimension can include a

**With IT operational data volumes at an all-time high and showing no signs of slowing in scope and complexity, IT executive leaders must embrace technologies like AI and Machine Learning.”**

– NANCY GOHRING, SENIOR ANALYST, 451 RESEARCH

number of different functions. Conclusions may be visualized or expressed in natural language for human consumption, or packaged into machine-readable form to be delivered across APIs. What is common to all of these is the need to translate findings into a form where action can be taken.

Communication via natural language was another major focus of the commercialization wave in the 1980s. At the time it had a strong rule-based flavor, with most algorithms capable of generating well-formed grammatical sentences in English. While this approach is still widely used, it increasingly competes with approaches that dispense with grammar and instead rely on large look-up and cross-reference tables. These latter approaches depend heavily on a lot of cheap, available computer and communications power.

## ► **AUTOMATION**

The fifth and final algorithm dimension of AI is automation, which is typically driven by history, context, or goals. “Automation” has been traditionally defined as combinations of hardware and software blindly carrying out a sequence of tasks that could be otherwise carried out by a human. One of the consequences of this kind of automation is

that an automated sequence of tasks, once underway, will carry on to its conclusion regardless of what is happening within its environment. If things start going awry, the only thing that can be done is for the executing sequence to be stopped in its tracks. Such a rigid approach is highly problematic in modern IT environments, which are in a state of almost constant flux as they adjust to changing business conditions.

Instead, automated response is feasible only if the task-execution sequence can be modified mid flight with new information. Knowledge may emerge about the event history (e.g. root cause), the context (e.g. current state), or the goals (e.g. modifying the purpose as a result of changes in the environment). This kind of flexibility is possible only with continuous communication of the results of on-going data selection, pattern discovery, and inference fed to the system.

These five algorithmic dimensions of AIOps taken together allow businesses to effectively support the IT systems driving digital business. Now let’s look at how the deployment of AIOps is likely to reshape the organization and processes that structure IT Operations.

# The Market Context for AIOps

## COMMERCIAL AIOps PLATFORMS

compete with six other software submarkets that roughly and conceptually align with the five dimensions of algorithms just discussed. Given the current size and promised growth of AIOps, it is not surprising that vendors dominating these submarkets will often attempt to extend their offerings with AIOps-like features. As a result, there can be confusion at the borders. A quick review of these six submarkets helps to demarcate them clearly from AIOps.

### ► LOG MANAGEMENT & DATA AGGREGATION

These vendors provide platforms primarily focused on ingesting logs and metrics into unstructured key-value databases where they are stored, accessed, and analyzed. The platforms have no built-in models of the environment from which logs and metrics are being drawn, which means that they differentiate on access and analysis. While this lends incredible scope and flexibility, it also means that users must approach the data with their own pre-existing skills and knowledge to correct for the platforms' lack of specificity.

## Log Management & Data Aggregation

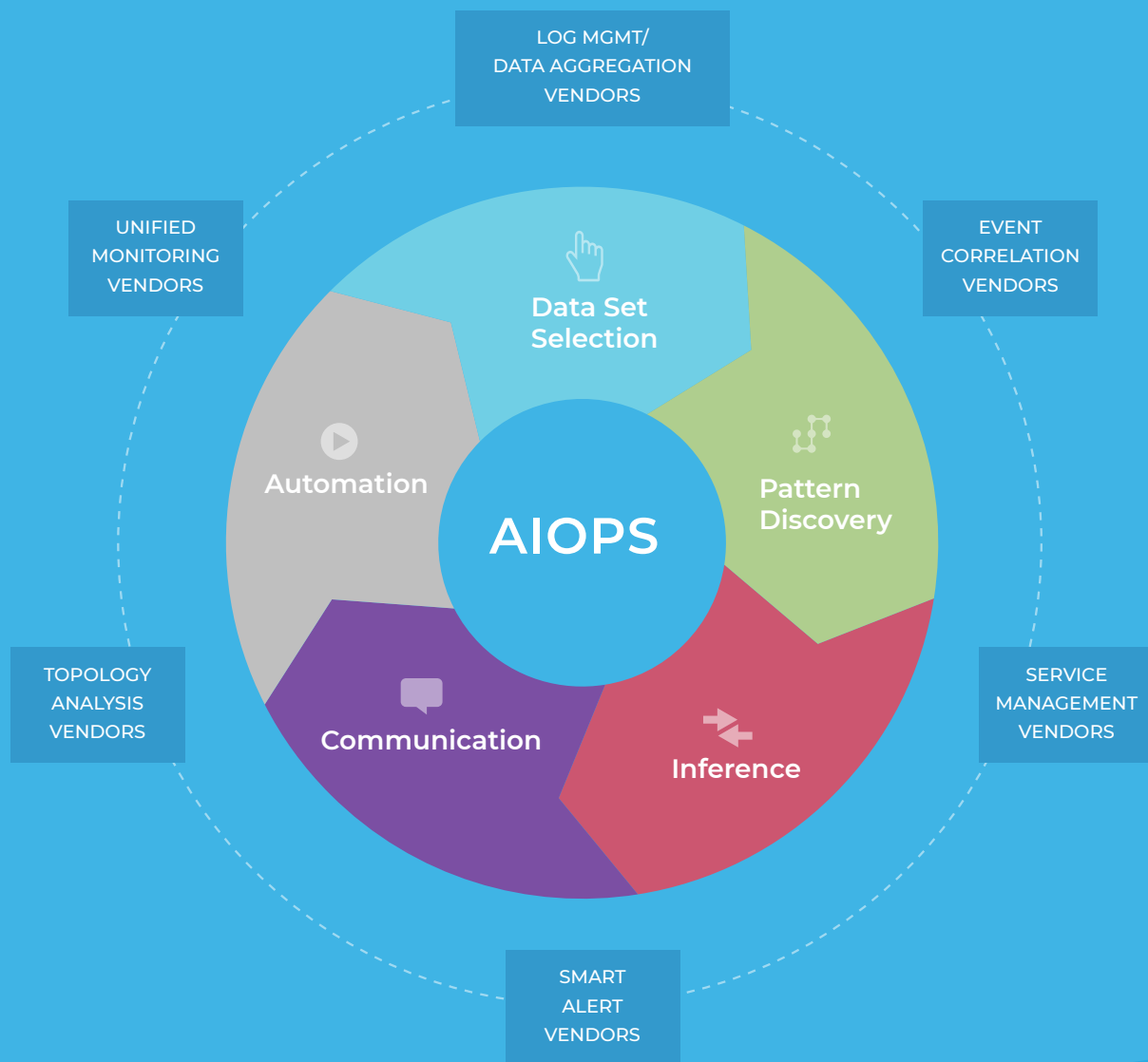
vendors have sought to enter AIOps by equipping their platforms with better visualizations, deeper statistical analysis, and ultimately, machine learning tool kits which allow for the automation of pattern discovery. They tend to fall short in two areas:

1. Users are required to work with historical data, while the complexity of modern IT systems demands at least the possibility of real time analytics.
2. The AI algorithms deployed are almost entirely confined to pattern discovery. Data selection and inference are largely ignored. Support for communications and automation are planned through partnership and acquisition.

### ► UNIFIED MONITORING

Vendors in this market originated in either application, infrastructure, or network monitoring. In recent years some have extended their capabilities through the acquisition of adjacent monitoring technology. Unlike the Log Management

## ADJACENT MARKETS



submarket, Unified Monitoring offerings are replete with domain specific knowledge and work in real time. Operators need to bring much less to the table in order to get value out of them. These vendors have sought to enter AIOps by adding both pattern discovery and rule-based inference to their offerings. One or both of these algorithmic

dimensions are deployed against the streams of performance and event data they capture. However these enhanced monitoring systems are limited by:

1. Their pre-existing domain knowledge is rigid and so, while it does provide some kind of data set selection

service, the tools are only able to work with well-understood and relatively static environments.

2. Like Log Management vendors, Unified Monitoring vendors view the communications and context-aware automation dimensions of AIOps as external to their core competency.

### ► **EVENT CORRELATION**

This submarket is one of the direct ancestors of today's AIOps market. The technology deployed sprung directly from the first wave of AI commercialization in the late 1980s. Vendors in this space offer platforms that use rules and logic-based inference to filter and group streams of event data, typically in the form of alphanumeric strings. Attempts to extend into AIOps usually involve little

more than making it easier to write and extend rules. The way these platforms work is fundamentally familiar to many IT Operations practitioners. They are easy to implement for simple and relatively static IT systems. Limitations include:

1. These platforms use functional restriction logic-driven inference. This means that it is difficult to create and maintain the thousands of rules required to capture and correlate complex IT system events.
2. Communications and context aware automation are not seen as integral to their offerings, similar to Log management and Unified Monitoring vendors.





## ► **TOPOLOGY-BASED ANALYTICS**

Platform offerings in this submarket can periodically discover components and connections constituting an IT stack, and then visually display the results. These were long a very popular feature of many ITOM software offerings. The topological or graphical relationships revealed by component connections can guide the discovery of root cause combating performance problems. Vendor attempts to extend into AIOps have taken two forms: either shortening the periods between topology updates, or automating root cause analysis inferences based upon path-tracing through graphs. With topologies linked to configuration management databases and other aspects of service management,

vendors in this space accept the centrality of communication and context-aware automation, even if they do not directly support those functions. However, the topology-centric approach is limited in two ways:

1. The relationships among events are only partially revealed through topology.
2. The automated support of path tracing is incapable of segregating correlation from causality, in most cases.



## ▶ SERVICE MANAGEMENT

Service Management, or “service assurance”, encompasses a broad range of technologies that include help desk platforms, configuration management and change management technologies, and workflow engines that support incident and problem management. Key to both the planning and execution roles of ITOM, many enterprises see these technologies as natural launching points for any kind of AIOps endeavor. There is a natural affinity for AIOps among these technology vendors, given the roots of help desk and CMDB technology in AI’s first wave. However, vendors in this market have been slow to make that expansion to date. When they have taken tentative steps, it’s either grafting rules-based event correlation into their portfolio of offerings, or adding further rule-based logic inferencing capabilities to their workflow engines and help desks. Two flaws mark most of these efforts, beyond their reliance on rules:

1. They fail to consider data that does not take the form of structured alpha-numeric text strings.
2. AI functionality is often too deeply wedded to workflows and processes that are highly rigid and centralized, undermining AIOps’ core purpose of handling rapidly changing, distributed environments.

## ▶ SMART ALERTING

Vendors in this space offer platforms that use rules and logic-driven inference to ensure that IT event notifications are routed to the right operators. Pursuit of the AIOps market has followed two complementary paths. First, some have introduced learning mechanisms so that alerts can be targeted more and more effectively, over time. Other platforms have added increasingly rich analytical capabilities that make use of both pattern discovery and inferencing at the point where events are first captured. This has brought them into direct competition not only with AIOps, but also with Event Correlation offerings. In general, these platforms fall short because of:

1. Reliance upon rule-based algorithms
2. A focus on structured event records
3. Inability to cope with large volumes of event data in the primitive unanalyzed forms generated by modern IT environments

While the market for AIOps platforms has emerged with its own distinct offerings, participants in six adjacent sub-markets will attempt to extend their offerings in the direction of AIOps in the future.

# The Challenges of Digital Transformation

A FUNDAMENTAL TRANSFORMATION in the nature of business has been enabled by critical changes in both organizations and their underlying technology. Taken together, these changes have allowed enterprises to create application and infrastructure stacks to more directly support and extend digital business processes. Moreover, they have ensured that these digital business processes can themselves change and evolve at breathtaking speed.

Of course, all of this has come with a price. While business agility and fitness have increased by orders of magnitude, the underlying IT systems have become dramatically more opaque and harder to manage. Let's examine the three root causes

of the blindness now faced by IT Operations professionals.

## ► SEPARATION OF IT SYSTEMS FROM BUSINESS PROCESSES

The mapping of the behavior of a business process in its execution to the underlying behaviors of IT system components has become abstract and indirect. In the past, IT systems supported and enabled relatively few business processes. The relationship between a system and the few business processes that it supported was relatively straight forward. Application or business logic resided logically and physically at one identifiable location in the infrastructure topology, while data resided at another identifiable location. Access was centralized

### Computing & Communications Technology Changes

- Shift to cloud-centered infrastructures
- Use of increasingly modular application architectures (culminating in container-based systems)
- Growing reliance on big data platforms
- Dominance of mobile, consumer-style application access interfaces

### IT Organizational Structure & Process Changes

- Emergence of DevOps as a set of principles organizing the relationship between the software development & IT Operations functions
- Increasing tendency to treat applications and infrastructure as an integrated programmable stack

and typically tethered to a desktop or workstation. When an incident occurred, a few data items about each location were usually sufficient to detect the source of the incident. Remedies could be applied through local fixes to assets over which the enterprise had direct control. Today's cloud services and dynamic programmable infrastructure mean that the IT system supporting and enabling a digital business process is spread out across components whose dimensions and locations are ever shifting. It's impossible to map an incident to a logical or physical location. Even if one could, the use of a public cloud compute and storage facility means that the access required to perform remediation is difficult to achieve without the right contractual terms and incontrovertible proof.

### ► IT'S BIG DATA PROBLEM

One of the key consequences of the heightened modularity of infrastructure and application stacks is the increased entropy of the data they generate. In the past, such stacks could be broken down into somewhere between five and ten large components. It was relatively easy to infer the state of the overall stack from a relatively small number of data items about each component. The choreography of the components was often so rigid that a modest



amount of data about one or two of them was sufficient to determine the source of almost any performance problem or incident. Now high levels of modularization due to object orientation and containerization have rendered the information extractable from component data highly localized. IT operators can no longer infer the state of the entire stack just from observing a small number of strategically selected data sources. Indeed, the only way of seeing today's application stack, let alone understanding and modifying it, is to analyze ever more data from the stack's constituent components. The ability



to make sense of this Big Data problem becomes virtually impossible without some kind of automated assistance.

### ► **FLUID & EPHEMERAL INFRASTRUCTURE**

Large chunks of most infrastructure and application stacks used to change slowly, if at all. The topologies of various components were rigid; their configuration remained the same from year to year, even decade to decade. The path from incident to cause was well understood in advance. Determining root cause was often just a question of

figuring out which path the disturbance had traveled. Today, modularization and cloud centricity have rendered interconnecting topologies very fluid, and the components of the stacks to be managed far more ephemeral. Cloud-based VMs can last only hours, while containers can last merely a microsecond. Paths from cause to effect have become more difficult to trace. Components may have vanished from the scene long before the source of the incident or issue can be ascertained.

# The Failure of Traditional ITOM Technologies

THE TRIPLE CHALLENGE OF digital transformation has rendered most monitoring, event, and incident management solutions obsolete at worst, or at least in need of major supplementation.

The inability of these three legacy monitoring technologies to handle modern IT systems--and the large, volatile and highly entropic data sets they generate – is what has spurred the rise of the AIOps market.

The growing significance of IT to digital transformation initiatives is precisely what is

leading global enterprises to pursue AIOps solutions at a rate of exceeding \$2 billion annually. The data sets required merely to observe what is happening, let alone find the source of issues and anticipate the future, are fueling its growth. The problem has simply become so large, so volatile, and so complex that AIOps has become a prerequisite for effective IT Operations in the 21st Century.

## Monitoring solutions

are tied to specific domains. Their ability to interpret the data they capture is entirely dependent on their a priori knowledge about the IT topology pre-built into them. They must locate elements taken from a very small subset of the data generated by applications, databases, networks, etc.

## Event Correlation

**solutions** require pre-written rules that determine which events deserve notice. Although less tied to specific domains, to be useful they require the environment being observed to have a static topology. Data sets need to be either small or highly redundant, or alerts will overwhelm the event management system.

## Incident Management


**solutions** presuppose a rigid topology and controllable event stream. They require that incident and problem resolution processes they support be well-defined, repeatable, traceable and deterministic.

# How an AIOps Platform Solves These Challenges

AT THE HIGHEST LEVEL, an AIOps platform combines logic-based and math-based artificial intelligence techniques in a manner that reflects the way the human brain actually works. Let's use this diagram of a typical AIOps workflow (*next page*) to examine how an AIOps platform copes with the triple challenge described above, working top to bottom.

First, the platform ingests streams of complex data generated directly from underlying IT system components or from existing monitoring, event, and incident management systems. Rather than relying on a static model to contextualize and interpret the data, it applies a collection of functions directly to the data itself to discover patterns that govern the behavior of the data stream. Ultimately it gains an actionable understanding of the IT environment on its own.

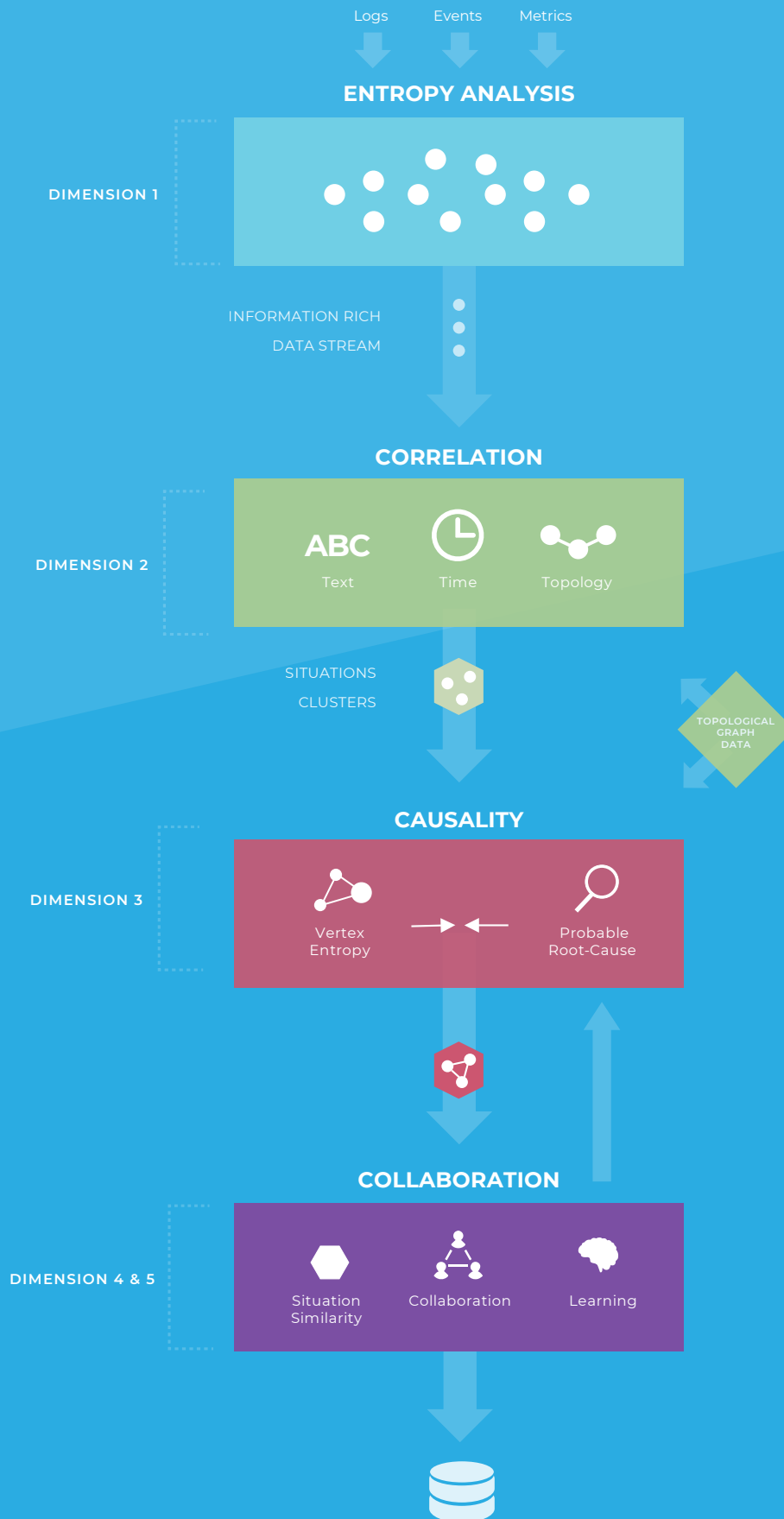
Next, data set selection algorithms are applied as data streams in. Data has many shapes and textures, so it needs to be translated into a form that can be worked upon by the rest of the system. Raw events are enriched by attributes that describe their



**AIOps technologies can help solve the immediate pain associated with IT Ops data overload, such as alert fatigue and slow mean time to repair, and enable business critical projects like digital transformation.”**

– NANCY GOHRING,  
SENIOR ANALYST, 451 RESEARCH

# THE AIOPS WORKFLOW





structure, typically using textual fields. The streams are then passed through a filter that attempts to exclude redundant events from consideration, leaving a significantly stripped down stream for further processing. Then, pattern discovery algorithms go to work. The platform tries to group event signals into meaningful groups that can be eventually tied to what impacts business process execution. AIOps groups or correlates events in three distinct ways: by proximity in time, in space (i.e. topology) or in textual attributes. The outcome of these three grouping functions is a cluster (i.e. a collection of what some vendors call incidents, situations, or scenarios), essentially packages of correlated events.

At the next step, inference algorithms are required. Correlations are immensely useful, returning indicators of a problem's root cause and grounds for future prediction. However, correlation is not causality. An IT Operations team can decide what actions need to be taken on system only when a causal connection between events can be firmly established. It is impossible to effectively automate IT Operations processes unless the robots or run-book execution platforms are fed actual causal

information. This ensures that problems are addressed efficiently and business process executions are optimized.

The platform now uses causal analysis to transform the correlational information present in the situations into causal information. Counterfactual reasoning eliminates all unlikely causes of the situation. Both temporal and topological information is applied to elicit the causal structure that underlies the correlations (e.g. time, topology, text) captured earlier. The results of causal analysis must then be communicated to both human and digital agents, where incidents can be resolved through context-aware automation. This layered process of ingesting and comprehending the meaning of events is but one workflow example, and not the only way of applying AI to IT Operations use cases. The fundamental architecture of AIOps, however, must be built upon the recognition that monitoring, event, and incident management in a digital business process setting has some foundational requirements. Namely, the ability to discover and analyze the patterns that emerge from a complex, ever shifting stream of data that itself reflects the ever evolving structures that constitute modern IT environments.

# The Bottom Line

- ▶ **The complexity of digital business** supporting IT systems has resulted in an ever growing volume of noisy data which needs to be taken into account by the IT Operations Management (ITOM) function.
- ▶ **AIOps requires the joint, coordinated deployments** of five distinct types or dimensions of algorithm: data set selection, pattern discovery, inference, communication, and context-aware automation.
- ▶ **AIOps links and integrates** the tasks performed by the four roles that constitute ITOM: observation, analysis, planning, and execution.
- ▶ **AIOps significantly reduces** the fixed costs and enhances the value of IT-related decision making.
- ▶ **Without the assistance of AI technology** across the spectrum of ITOM, it has become impossible to observe, understand, and modify IT systems in support of digital transformation imperatives.

## FEEDBACK ON THIS PAPER?

Submit your comments to the authors at  
[INFO@AIOPS-EXCHANGE.ORG](mailto:INFO@AIOPS-EXCHANGE.ORG)

## ABOUT THE AUTHORS

### Will Cappelli

Will studied math and philosophy at university, has been involved in the IT industry for over 30 years, and for most of his professional life has focused on both AI and IT Operations Management technology and practices. As an analyst at Gartner he is widely credited for having been the first to define the AIOps market. Will is currently CTO, EMEA and VP of Product Strategy at Moogsoft. In his spare time, he dabbles in ancient languages.

### James Governor

Founded RedMonk in 2002 with Stephen O'Grady. We focus on developers as the real key influencers in tech. Understanding that people choose technology because of gut instincts not facts per se. An ex-journalist, I have managed teams and news agendas in weekly publication grind. IBM and MS watcher since 1995. Goals—build RedMonk. Specialities: Developers, developers, developers.

### Clive Longbottom

Clive Longbottom is founder of Quocirca and is a highly respected and globally recognized industry analyst, covering a range of business and technology areas. Clive's primary coverage area is business process facilitation, where he covers the need for companies to understand their core processes across their value chains, and the technologies that should be used to facilitate them in the most flexible and effective manner.

## ABOUT THE AIOPS EXCHANGE

AIOps Exchange is a private, not for profit forum committed to the open exchange of ideas, trends, and best practices defining the future of AIOps. IT industry thought leaders, influencers and C-level executives come together at our invitation-only events to share their insights on the best use of artificial intelligence in enterprise IT Operations. AIOps Exchange is committed to the private exchange of ideas on trending topics such as digital transformation, service assurance, and business agility. No product pitches. No sales people. No press. AIOps Exchange participants are defining the future of AIOps while helping each other to scale and accelerate business growth.



[www.aiops-exchange.org](http://www.aiops-exchange.org)