AIOPS VS. OBSERVABILITY DILEMMA: WHICH ONE IS BETTER?

AIOps vs. observability dilemma: which one is better?

The term observability has been around for over 10 years, but in the last three to four years, the concept has caught fire, albeit without sufficient guidance. That has led to tool sprawl, and now, in large enterprises, it is not uncommon to have 15 to 20 observability tools (and yes, even the old-style monitoring tools have been rebranded to observability, too). There are too many signals for IT to sift through, and they're overwhelming IT teams across large enterprises. How do you make sense of all these signals when you're dealing with a major incident?

For IT leaders, applying the appropriate technology to the task at hand becomes imperative when dealing with all the noise, complexity, rapid changes, and fast-paced innovation. When it comes to AIOps and observability, which approach makes the most sense for your business—or do you even have to choose?

Not necessarily, if you implement the right AIOps solutions in your environment. Here, I will explore the two approaches to help you determine whether AIOps or observability will help you achieve your IT operations (ITOps) and business goals. To dive deeper, check out our *AIOps Is Not Observability* whitepaper or the video interview with Carlos Casanova, a principal analyst at Forrester, below.

AIOps and Observability Defined

Artificial intelligence for IT operations, or AIOps, uses AI and machine learning (ML) to automate IT Ops, from reconciling and analyzing data collected by various sources—including observability tools—to conducting [root cause analysis](#) and automated remediations. AIOps is a prescriptive and proactive means to direct IT teams to the source of problems with high confidence and context, ultimately reducing or eliminating the time spent troubleshooting an issue.

AIOps can take in volumes of data (from observability tools or natively), reconcile and normalize it, and provide a unified view (east-west) across IT domains—proactively pointing IT to the source of problems and often preventing an incident from becoming a business-impacting problem. AIOps focuses on automatic problem resolution when problems do occur and preventing emerging potential incidents from happening.

On the other hand, observability tools also collect massive amounts of data to help IT teams infer the state of their observable systems. With this data, IT practitioners can query the data to iteratively troubleshoot and build awareness of the systems' state from the data. Observability can be critical to gain insights into the performance of distributed systems, and often requires knowledge of query languages (such as PromQL, or others) to quickly interrogate all the collected data.

Key differences

The differences between AIOps and observability can be boiled down to the following:

- AIOps reconciles ingested data and delivers a unified view (east-west) across disparate tools and domains versus observability tools being used to explore data after a problem occurs and within the observability domain (north-south), often isolated from other observability domains.
- AIOps focuses on automatic problem resolution and preventing incidents from happening versus observability tools, which enable data exploration
- AIOps provides noise reduction and root cause analysis versus observability data, which is used for interactive exploration
- AIOps focuses on automation and intelligent remediation using AI/ML versus observability, which focuses on data collection and investigation.
- AIOps uses predictive algorithms to optimize service assurance versus observability, which uses capacity planning purposes in semi-automated ways.
- AIOps systems provide best action recommendations based on the past and in real-time, ML-driven insights versus observability, which provides explorative iteration.

How AIOps Drives Value for IT

Enterprise IT organizations today are already seeing the gains of applying AIOps across their environments using BMC solutions.

BMC's AIOps is powered by its [composite AI](#), including causal, predictive, and [generative AI (BMC HelixGPT) solutions](#), which automate traditional incident analysis and offers a clear, plain-language summary of the problem—along with information on how the same type of problems was solved in the past.

Using composite AI, an AIOps solution can [detect an anomaly](#), generate a summary of the incident, and suggest a best action recommendation (BAR). Automated incident resolution with AI and

generative AI (Gen AI) prevents downtime and allows IT to perform health checks preemptively, improving overall system reliability and resilience.

AIOps can also accelerate troubleshooting workflows by providing predefined prompts to answer questions that lead to better understanding of complex systems, and ultimately, faster resolution. Using a solution such as Ask BMC HelixGPT speeds up the process and results in quicker resolutions.

Gen AI in AIOps solutions such as BMC Helix helps IT teams confidently conduct changes, mitigating the risk that a change will negatively impact the environment. Our AIOps approach, coupled with ServiceOps, enables flexible change risk management and automated or hybrid change governance.

AIOps can also use its knowledge of historical usage patterns and business trends to accurately predict future resource demands. This helps prevent outages and optimizes operations by allowing enterprise IT to run what-if scenarios to right-size capacities for user demands. In this scenario, AIOps helps organizations proactively plan for capacity, ensuring both performance and cost efficiency.

AIOps Drives Value for Observability

IT teams could achieve greater benefits from aggregating observability data into their AIOps solution. AIOps delivers true value for observability and helps enhance this understanding with AI/ML-driven automation and predictive and proactive (preemptive) capabilities, allowing IT and the business to make informed decisions. AIOps enables IT teams to scale and be more productive and support a much greater number of complex systems.

Observability tools provide an abundance of signals to IT teams, and AIOps synthesizes those signals to determine a root cause and provide a BAR based on ML. Observability is important for gaining insight into the performance of distributed systems, while AIOps helps enterprises achieve better business outcomes through intelligent operations and context.

As observability data becomes more critical across highly distributed, sophisticated environments, AIOps steps in to make sense of the noise, pinpoint the problems or prevent them, and enable IT to improve service reliability and deliver exceptional user experiences.

To summarize: AIOps is not observability, AIOps drives value for observability. So, which one is better? That depends on the outcomes you want to achieve.

Learn more in white paper that digs deeper into AIOps and observability here.