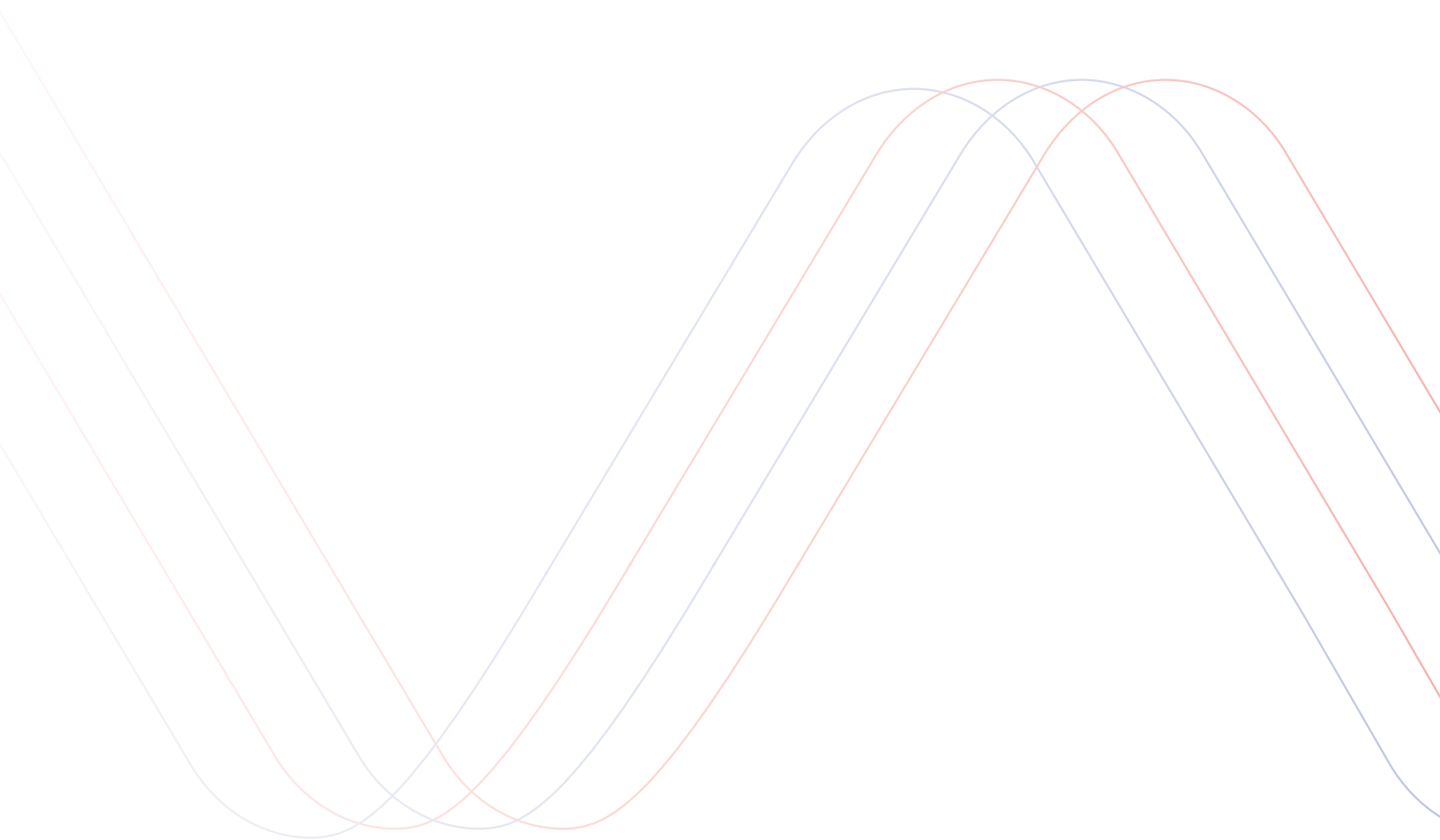


AI Ops is not observability

AI Ops drives value for observability.

Table of contents

- 03** Executive summary
- 04** How we (BMC) define AIOps and observability
- 05** How is AIOps different than observability?
- 07** How IT teams use AIOps (use cases)
- 08** Why is AIOps more valuable than just observability?
- 09** Summary: AIOps drives value for observability



Executive summary

Over the last 10 years, we've witnessed a rise in observability solutions. This evolution from monitoring to observability was natural, driven by the needs of modern software delivery architectures. It required a shift in our approach to monitoring, moving away from understanding only discrete components at specific points in time.

The adoption of modern software delivery and distributed systems created the need to ingest and manage vast amounts of data through observability. As the adoption of observability grows, IT must deal with an unprecedented amount of data. Every application, infrastructure, and network across complex hybrid environments produces digital exhaust, generating data at overwhelming speeds and in different formats. This raises the question: how do IT teams manage all this data? IT teams need to improve and enable business operations. Is observability enough? And not only to make sense of all of it, but also connect it with the broader business operations.

While observability has become important for empowering IT practitioners to ask any question of the data based on their understanding of the system's current internal state, that is not enough. This is because there are too many observability tools typically in use; there still too many alerts generated across complex environments; and overall, there is too much observability data that IT, including IT operations (ITOps), DevOps, and site reliability engineering (SRE)

teams need to sift through to get to the root cause of the issue. What is often missing is the vital context needed to make the best and fastest informed decisions, both manual and automated.

What IT teams need is AIOps (artificial intelligence for IT operations). AIOps is crucial for helping IT distill signals from the noise, within the context of that moment in time, based on historical operating scenarios, to help them get to the root cause quickly. It allows them to move from being reactive to proactive via risk assessment prior to changes. It allows IT to make actionable decisions from all the observability data to preemptively remediate an issue based on understanding prior trends. As such, AIOps drives value for IT teams seeking to get a handle on all that data and achieve self-healing operations.

In this white paper, we'll explore the next step in the evolution from observability to AIOps and the relative value of two approaches. But first, let's start with definitions and our view of what observability and AIOps are.

How we (BMC) define AIOps and observability

Observability

Observability tools collect large amounts of data to help IT infer the state of the observable system. IT practitioners can ask any question of the data to troubleshoot and build awareness of the IT systems' state from that data. With these insights, IT can continue to iterate and explore data with queries to ultimately converge on the source of the problems. Typically, observability solutions require knowledge of query languages (such as PromQL, or others) to quickly interrogate all the collected data.

AIOps

AIOps solutions use artificial intelligence and machine learning (AI/ML) to automate ITOps. These solutions analyze data from multiple monitoring and observability tools conducting root cause analysis (RCA) to quickly help find the root cause of issues and recommend remediation. These solutions collect data from across the IT estate, either natively or, more commonly, through intelligent collectors that bring in data from other observability and monitoring solutions, such as networking and application performance management (APM) solutions.

AIOps solutions also can automatically ingest topology data or build and maintain a dynamic topology of all hardware, services, and software running in IT environments. This dynamic mapping allows AIOps tools to run composite AI/ML, including causal, predictive, and generative AI, to assist IT with intelligent decision-making, such as identifying the root cause of a problem.

In addition, AIOps solutions provide critical context that is often lacking when observability tools are deployed on their own. The AIOps solutions derive this context from cross-landscape visibility and analytics that provides that context. As a result, there are expanded possibilities of automation, remediation, proactiveness (in incident prevention), and predictability.

It doesn't stop there; AIOps also ingests data from IT service management (ITSM) tools, such as incident data and changes, as well as from continuous integration and continuous deployment (CI/CD) tools and pipelines, such as Azure DevOps. AIOps not only ingests data, but also normalizes and reconciles it (such as when host names are defined differently in IT infrastructure tools compared to APM tools).

How is AIOps different than observability?

Now that we have definitions, let's explore how AIOps is different from observability.

- **AIOps reconciles ingested data and delivers unified view across disparate tools and domains (proactive versus reactive)**

AIOps platforms integrate data from various IT tools, APM, observability, network monitoring, CI/CD systems, ITSM tools, infrastructure management, and more. This unified view breaks down silos and provides comprehensive insights. The important difference from observability solutions is that AIOps reconciles data and uses the integrated view, combined with topology information, to feed AI/ML models. As a result, AIOps is prescriptive and proactive and helps direct IT teams to the source of the problem with high confidence and context, helping reduce or eliminate the time spent troubleshooting. Some AIOps solutions natively ingest observability data, as well such as metrics or log data, which is the case with BMC Helix ITOM.

- **AIOps focuses on automatic problem resolution and preventing incidents from happening (automation versus data exploration)**

Observability focuses on gathering data such as logs, metrics, and traces from the environment to help IT infer the state of the system and perform iterative troubleshooting after an issue occurs.

This approach can be seen as reactive or forensic. For instance, if a metric detects a sudden spike in the CPU load, an observability solution would typically create an alert for a site reliability engineer (SRE) to troubleshoot and investigate. That alert then assists the SRE in triaging the issue or digging deeper into application or other log data to converge on the solution. This process requires manual effort.

Unlike observability, an AIOps solution typically uses AI/ML to identify patterns and anomalies in real time, predicting potential incidents before they impact the business. AIOps tools learn from historical resolutions as well as historical patterns and trends within the normal operation of the environment and help IT teams automate problem resolution. Additionally, an AIOps solution continuously evaluates the system and updates topology maps dynamically, continually understanding system performance and flagging potential issues with high confidence. This helps improve the system's reliability and responsiveness.

- **AIOps provides noise reduction and root cause analysis (versus offering observability data for interactive exploration only)**

AIOps platforms ingest, reconcile, and normalize vast amounts of data from different domains and tools. Unlike observability tools, which collect and store data for interactive exploration by humans, AIOps solutions typically combine topology discovery and/or ingestion with AI/ML. These tools automatically surface issues, detect patterns, and flag potential root causes. This is possible because of the context these tools have based on previous situations and scenarios relative to when a potential pattern is detected. These insights are dynamically updated and continuously evaluated by ML.

With continuous insight into the dynamic state of the systems, AIOps filters out noise and correlates events across multiple systems. By applying causal AI, AIOps identifies the root cause of issues with high probability, helping IT teams reduce or eliminate alert fatigue or alert storms.

- **AIOps focuses on automation and intelligent remediation using AI/ML (versus collecting data and iterative investigation)**

By applying causal, predictive, and generative AI and automating issue resolution, AIOps frees IT teams from manual work, allowing subject matter experts (SMEs) to focus on strategic initiatives. By using AI/ML-powered situation recognition (event clustering), AIOps reduces noise, allowing IT, networking, and

developer teams to focus on critical tasks. Moreover, because it remembers previous situational resolutions, features like situation fingerprinting learn from past incidents to identify similar situations, expediting resolutions based on historical data. Essentially, AIOps solutions maintain critical context needed for successful resolutions.

AIOps platforms can automatically execute predefined actions such as scripts from runbooks and playbooks in response to detected issues. This includes restarting infrastructure components, clearing file caches, adding capacity during busy times, or rerouting traffic, significantly reducing response times.

- **AIOps optimizes service assurance (versus manual or semi-automated capacity optimization)**

Using predictive algorithms, AIOps solutions enable proactive forecasting of resource saturation, preventing outages before they occur. Through what-if business planning and simulation, IT teams can accurately predict and optimize costs and right-size resources for efficient operations. By analyzing historical data, AIOps can predict potential system failures or performance degradation, enabling preemptive actions.

- **AIOps fosters intelligent decision-making (versus explorative iteration)**

AIOps systems can recommend the best course of action based on data analysis, past incidents, and ML models. This intelligent decision-making supports faster and more accurate issue resolution.

How IT teams use AIOps (use cases)

Now that we have learned important differences between AIOps and observability, let's explore how IT teams use AIOps.

01

Automating resolution using AI and generative AI

Using generative AI, such as BMC HelixGPT, allows IT teams to provide a best action recommendation (BAR) for incident resolution. For instance, when an anomaly is detected, the AIOps system, based on historical knowledge, can generate a summary of the incident and suggest a BAR. Please see a few applications of BAR from our recent [blog](#). This proactive approach prevents downtime and allows IT to perform health checks preemptively, improving the overall system reliability and resilience.

02

Accelerating troubleshooting workflows with generative AI

In addition to automated remediation, AIOps solutions accelerate troubleshooting workflows. For instance, a solution such as Ask BMC HelixGPT accelerates the troubleshooting workflow by providing predefined prompts to answer questions that lead to better understanding of complex systems and faster remediation.

03

Using generative AI for proactive change risk management and confident deployments

Beyond summarizing and providing BARs, AIOps solutions such as BMC Helix ITOM help IT accelerate change management and mitigate risk using BMC HelixGPT, which allows DevOps and IT teams to confidently predict successful deployments. Our AIOps and ServiceOps approach allows for flexible change risk management and automated or hybrid change governance, including waterfall and agile/DevOps practices.

04

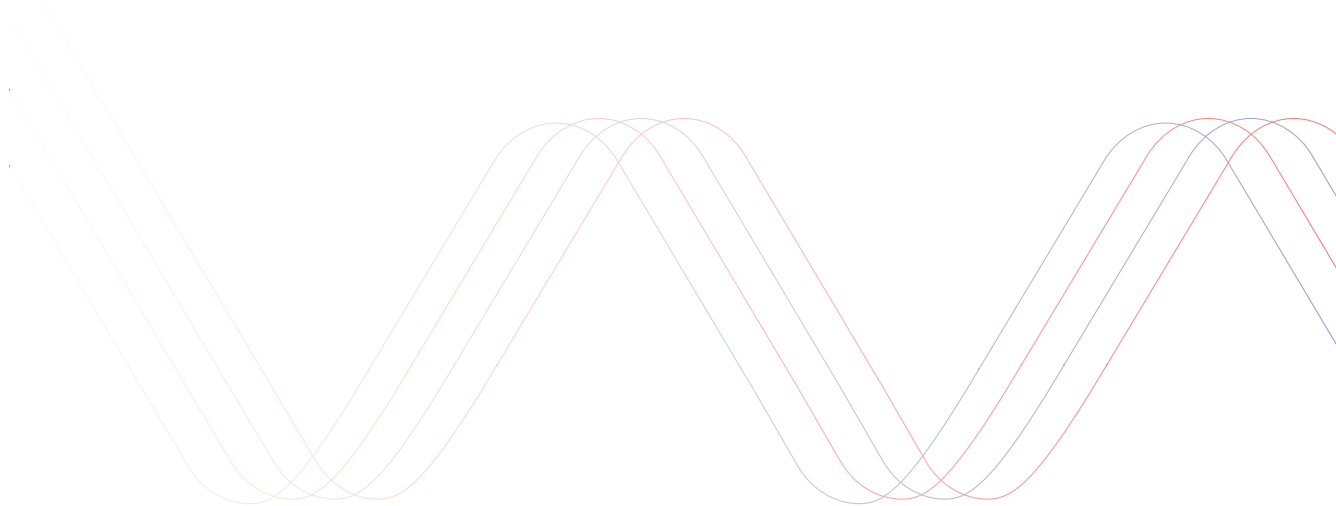
Preventing outages and optimizing operations using service assurance

AIOps can predict future resource demands based on historical usage patterns and business trends. It allows enterprises to run what-if scenarios to right-size capacities for user demands. This helps organizations proactively plan for capacity needs, ensuring optimal performance and cost efficiency.

Why is AIOps more valuable than just observability?

AIOps is more valuable than just having observability because it enables ITOps teams to scale and be more productive. It allows them to support a much greater number of complex systems, and many more system changes associated with rapid innovation and digital transformation. Observability solutions provide the data—often an overabundance of data—as well as its corresponding alarms and noise, to the ITOps teams. AIOps helps to synthesize that data, distill the root cause, and recommend remediation. This helps to reduce the mean time to repair (MTTR) and increase the reliability of services.

AIOps helps to identify risk before changes, thereby proactively preventing incidents and improving the effectiveness and efficiency of the network operations center (NOC) and the rest of the ITOps team.



Summary: AIOps drives value for observability

Observability is important for gaining insight into the performance of distributed systems, whereas AIOps delivers true value for observability and helps enhance this understanding with AI/ML-driven automation and predictive and preemptive capabilities, allowing IT and the business to make informed decisions. Ultimately, AIOps helps enterprises achieve better business outcomes through intelligent business operations, empowered by continuous optimization of capacity to support increased customer loads based on detected patterns.

AIOps solutions look horizontally (east-west) across systems and the entire IT landscape. These tools go beyond just having a vertical (north-south) focus on isolated systems, with no context and no learned patterns or knowledge of adjacent systems. As such, AIOps powers AI/ML-driven automation, problem resolution, and unified insights,

enabling organizations to manage complex IT environments more efficiently and effectively. Together, they create a comprehensive solution for modern IT operations.

As the appetite for observability solutions and data grows, IT teams can become inundated and overwhelmed with data. Therefore, as enterprises demand more observability, AIOps becomes increasingly necessary to make sense of all the data.

AIOps plays an essential role in enhancing service reliability and resilience, improving self-healing, and delivering exceptional user experiences. For enterprises looking to stay ahead in the competitive digital landscape, embracing AIOps is not just an option—it's a necessity.

To learn more, visit bmc.com or contact sales.

About BMC

BMC empowers 86% of the Forbes Global 50 to transform digital operations into opportunity. Our leading portfolio of AI-enabled software connects data, automation, and observability across the business, enabling each customer to become an Autonomous Digital Enterprise ready to seize competitive advantage in a world of constant change.

www.bmc.com



BMC, the BMC logo, and BMC's other product names are the exclusive properties of BMC Software, Inc. or its affiliates, are registered or pending registration with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other trademarks or registered trademarks are the property of their respective owners. ©Copyright 2024 BMC Software, Inc.



* 5 4 8 0 7 0 *