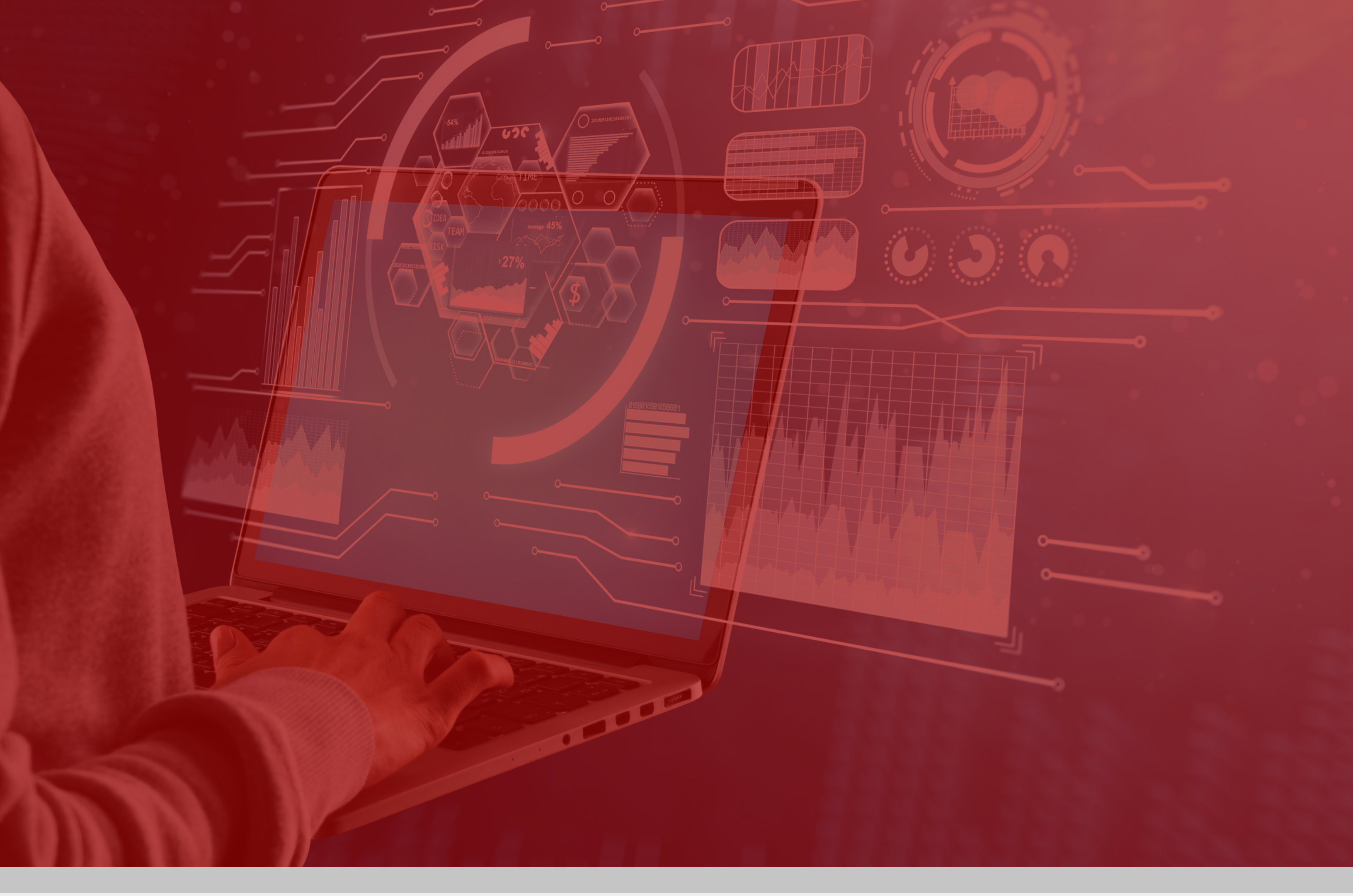

WHITE PAPER

technologies
A Broadcom Company

The Definitive Guide to AIOps

Table of Contents

Introduction

Over the past several years, IT teams have confronted a dizzying array of new challenges. Individually, these challenges have been easy to overlook. But collectively, they have generated a paradigm shift in the way organizations must monitor and manage their IT environments.

This shift results from a confluence of several factors. One is unprecedented customer expectations. In a world where 40 percent of consumers will abandon a website that takes more than three seconds to load,[1] and when a mere 5 percent difference in customer loyalty can translate to a revenue change of as much as 95 percent,[2] IT teams are under enormous pressure to optimize application performance and reliability for customers.

Complicating matters further is the fact that engineers must also support workforces that, over the course of the COVID-19 pandemic, have become increasingly distributed. Like consumers, employees expect a seamless, high-performing experience, even when they work remotely.

> The environments that IT teams must manage in order to meet customer and employee satisfaction have never been as complex as they are today.

At the same time, the environments that IT teams must manage in order to meet customer and employee satisfaction have never been as complex as they are today. More than 90 percent of enterprises now use the cloud to host at least part of their workloads.[3]

A majority of IT organizations also deploy applications using containers and microservices, often within scale-out, software-defined environments. While these technologies can improve the performance of applications as well as increase the velocity of software delivery, they create IT environments that are characterized by an unprecedented degree of complexity, making it harder than ever to find and fix performance and reliability issues.

Meanwhile, even the tool sets that IT teams have adopted to help manage performance and reliability pose their own challenges. It's common today to rely on a complex series of monitoring solutions. Each team or unit within the IT organization may have its own set of tools, and it is often necessary to use different tools for different types of environments: each public cloud has its own native monitoring tools, for instance, which teams may need to use in conjunction with third-party solutions that can also monitor on-premises environments. Indeed, according to the 2020 report "Using AIOps to Gain Observability and Insight," which was prepared for Broadcom by Dimensional Research, more than half of organizations currently use at least six observability tools.[4]

[1] Neil Patel, "**How Loading Time Affects Your Bottom Line**"

[2] Hubspot, "**Here's Why Customer Retention is So Important for ROI, Customer Loyalty, and Growth**," Sophia Bernazzani

[3] Hosting Tribunal, "**Cloud Adoption Statistics for 2021**," Nick Galov, January 19, 2021

[4] Dimensional Research, sponsored by Broadcom, "**Using AIOps to Gain Observability and Insight**," November 2020

What all of these tools mean is that monitoring data and workflows tend to be siloed and complex, making it challenging to gain a clear understanding of the state of the IT environment and its relationship with business outcomes.

AIOps as the Answer to Complexity

Faced with this dizzying array of challenges, how can modern IT teams efficiently and effectively monitor software environments?

The root of the answer is artificial intelligence for IT operations, or AIOps. In recent years, AIOps has emerged as a better solution to the challenge of ever-increasing complexity in IT. AIOps leverages big data, data analytics, and machine learning to provide insight and enable a higher level of automation (one that does not depend extensively on human operators) for the management tasks that modern infrastructure and software require.

AIOps is playing an increasingly key role in enabling new efficiencies for IT teams. It makes it practical to adopt complex next-generation technologies that cannot be managed successfully using traditional solutions, while also guaranteeing superlative performance and reliability to end-users.

> In short, businesses of the future won't survive without the assistance of AIOps.

In short, businesses of the future won't survive without the assistance of AIOps. If your business has not yet begun adopting AIOps-powered solutions, now is the time for assessing, planning, and implementing AIOps tools that can drive business value.

This guide is designed to help you in your journey toward AIOps adoption. It defines AIOps and assesses the current state of AIOps within the IT industry. It also identifies and explains the core components that drive an AIOps solution, as well as the main use cases for AIOps-powered tools.

Chapter 1: What Is AIOps?

Defining AIOps

AIOps is the use of machine learning, big data, and automated decision-making to complete IT tasks. AIOps makes it possible to automate processes that would traditionally require significant manual intervention by humans.

AIOps, which is short for "algorithmic IT operations" or "artificial intelligence for IT operations," entered the IT lexicon in 2016, when Gartner coined the term as part of an effort to understand how data analytics was enabling new efficiencies for ITOps teams.

Why Is AIOps Innovative?

Artificial intelligence is not new. Neither is the use of analytics to help drive IT operations, an established practice known as IT operations analytics, or ITOA.

What has changed in recent years with the emergence of AIOps, however, is that the advent of modern cloud computing and big data processing solutions has finally made it possible to leverage AI systematically as a means of optimizing IT operations. Whereas data analytics were previously of limited use for IT teams due to processing constraints, AIOps now provides IT engineers with access to tools that can make advanced decisions and perform automated actions in real time by systematically collecting and analyzing data.

AIOps thus represents a much more refined, sophisticated way of integrating data analytics into ITOps. In addition, it helps traditional ITOps admins transition into site reliability engineering (SRE) roles and support more scalable workflows that align with business needs.

The Evolution of AIOps

Since its inception in 2016, AIOps has evolved from a nice-to-have or cutting-edge type of tool to an essential component of any observability strategy.

As of November 2020, 25 percent of organizations surveyed by Dimensional Research were already using AIOps, while another 59 percent have plans to implement AIOps.

What's more, AIOps is helping teams get the most from SRE, a strategy for increasing application quality and reliability. The percentage of companies surveyed by Dimensional Research that are already using SREs or have plans to add them to their team correlates closely with the number of organizations that have adopted AIOps or plan to do so in the future.

The takeaway is that investment in AIOps is not an anomaly or a one-off technological change. It has become a core component of a broader commitment to increasing automation and reliability across businesses of all types. Indeed, you might say that AIOps has become the linchpin in the latest phase of digital transformation.

Core Components of AIOps

Businesses seeking to capitalize on AIOps as part of IT modernization must base their AIOps strategy upon three core components.

The first is observability. Observability means the ability to collect data from all layers of the software environment in order to provide deep visibility into what is happening within each layer while also revealing the overall state of the environment as a whole. It also enables engineers to understand the relationship between individual components and end-to-end system health. By allowing teams to understand the internal state of complex systems using data sources (such as logs and metrics) that can be collected from the surface of those systems, observability enables the visibility that AIOps tools require to identify and evaluate problems.

Second, AIOps requires aggregation, correlation, and analytics. It's only by interrelating observability data from multiple sources and analyzing it comprehensively that AIOps tools can identify meaningful trends within the data—including complex patterns that human engineers working manually would be unable to recognize.

Finally (and most importantly), AIOps requires automation. AIOps tools automatically determine the root causes of problems within software environments, then plan and execute remediations for them. The ability to identify the origin of and fix complex problems automatically, without having to wait on human engineers, is the killer feature of AIOps. Automation not only enables faster resolution, but also increases consistency and predictability. Different humans might respond to the same problem in different ways, but AIOps is consistent and methodical.

AIOps Use Cases

AIOps can be applied to virtually any workflow or challenge facing modern IT teams.

Among the most common use cases for AIOps are improving application service levels and performance by automatically managing alerts and responding to service quality problems. This category of use case is especially important in contexts involving highly complex software environments in which human engineers would struggle to know which alarms to prioritize and how to track down root causes within distributed, multi-layered environments.

At the same time, AIOps can also be applied to even more complex use cases, such as optimizing software performance over time. Rather than merely responding to issues as they arise, AIOps tools can proactively make predictions about resource optimization opportunities, emerging performance problems, and so on. They can then take action automatically based on the insights they identify.

This is only an overview of the potential use cases of AIOps. Subsequent chapters offer full context into applying AIOps in practice by identifying the most relevant use cases for AIOps within your business and supporting AIOps initiatives successfully.

Chapter 2: Data Collection and Observability: From Chaos to Information

The previous chapter touched on the importance of data collection and observability as one pillar of AIOps. Given the complexity of this topic—and the considerable challenges IT teams face in actually translating data into observability—it's worth diving deeper into this area.

Modern software systems generate dizzying volumes of data. The key challenge when it comes to observability lies not in finding data, but in taming it in such a way that it is actionable and optimized for driving AIOps workflows.

In order to achieve observability, IT teams must address four key priorities related to data collection and analysis.

Disparate Completeness

Data sources for observability come in many shapes and sizes. Some might be conventional application logs that are written to persistent storage, which are straightforward to collect and analyze. But engineers may also need to collect logs from inside containers, where log data is not stored persistently. Events or metrics may also disappear if not collected in real time and aggregated within a persistent storage location.

Making matters more complicated is the fact that data types vary widely. Different logs use different formats. Some events and metrics data is structured in standardized ways, while others are produced haphazardly. Data is often timestamped, making it easy to analyze using a time-series approach, but that is not always the case.

> The key challenge when it comes to observability lies not in finding data, but in taming it in such a way that it is actionable and optimized for driving AIOps workflows.

In short, observability data is disparate and siloed. To achieve full observability, teams must collect all data available to them—not just the data that is easiest to ingest and analyze—and then transform it in such a way that it can be processed consistently and efficiently.

Data Veracity

Not all data is necessarily accurate or actionable. Data that was not collected in real time may no longer be relevant by the time it is analyzed. Some data, such as logs from containers that are no longer running, may reflect the state only of systems that are outdated. In other cases, it is difficult to extrapolate from one type of data source (such as application data) to glean insight into another layer of the environment (such as your infrastructure).

What all of this means is that, in order to drive observability and AIOps, data must be accurate and normalized to the full extent possible. AIOps can help validate and clean data in many cases, but AIOps tools nonetheless require relevant data to perform their work. Teams must therefore be able to recognize the limitations within their data and use that insight to inform the way they deploy AIOps tools.

Data Context

On their own, individual data sources are of little value. Knowing that a Kubernetes Pod restarted, or that a software-defined storage system became unavailable, means little if those events cannot be correlated with what was happening on physical servers, virtual machines, operating systems, CI/CD pipelines, and every other layer of the software stack.

That's why it's critical to be able to correlate and contextualize data to achieve end-to-end visibility across the software environment, and from the top to the bottom of the software stack.

Data Openness

A final key factor to consider when preparing data collection and normalization solutions for AIOps is the issue of data-agnosticism. That means the ability of an AIOps tool to work with any type of data and apply it to solving problems in any domain.

Data-agnostic AIOps solutions are superior to tools that require a certain type of data, or that can address only a certain range of challenges. The latter solutions can lead to lock-in and restrict your business's ability to modify its AIOps toolset and processes in the future. In contrast, open solutions enable a data-agnostic approach to AIOps. They allow teams to work with whichever data sources are available to them, and to evolve their observability strategy seamlessly along with their IT environment.

Some such platforms are more "open" and compatible with third-party tools than others. If you consider commercial tools for data collection and normalization, assess how suitable they are for enabling a data-agnostic approach.

Chapter 3: Applying Analytics: From Information to Insights

The previous chapter discussed which kinds of data drive AIOps workflows, and how data must be managed to deliver full observability. Now, let's take a look at how AIOps derives insights based on data and observability.

At first glance, the focus of AIOps may seem to be about detecting anomalies within data sets that could indicate a problem. But in reality, problem detection is only part of the equation. What really makes AIOps powerful is its ability to surface actionable insights that help teams remediate problems—or, in some cases, allow AIOps tools to perform remediation automatically.

To deliver fully on its promise, then, AIOps must apply data analytics in a way that both detects and solves problems. Several principles undergird this functionality.

Topology

Given the disparate data sources at play in an AIOps workflow, being able to map data to the systems it represents—a process known as topology—is central to effective analytics. Merely knowing that an event happened somewhere within a system is not enough. You must understand where the event occurred, which corresponding events happened in other parts of the system and how the events impacted the collective performance of the system and business as a whole.

Because modern IT environments are large, complex, and constantly changing, building topologies manually is not feasible. AIOps tools must therefore be able to map data and analytics to complex systems automatically and continuously, updating their insights as the system changes and evolves.

Actionable Analytics

Performing analytics for analytics' sake offers little value. In order to make a meaningfully positive impact on system performance and end-user experience, the analytics at the core of AIOps must produce actionable, tangible outcomes.

There are a variety of ways in which AIOps tools can do this. Common examples include:

- **Alarm management**: Faced with a never-ending stream of alerts, IT teams can quickly become overwhelmed. AIOps tools can analyze complex patterns within alarm data sets, and correlate alarm data with other data collected from the environment, to triage alarms and identify false positives to reduce alarm noise. The result is more efficient and more effective alarm management.
- **Root cause analysis**: In modern IT environments, tracing surface-level issues to their root cause can be very difficult. Finding the particular microservice that is causing a delay in application response, for instance, is challenging when the application includes a dozen, let alone hundreds or more, microservices. By correlating data from multiple sources, AIOps can make accurate determinations about complex root-cause issues.
- **Prediction and optimization**: As noted above, AIOps is not just about solving existing problems. It also helps teams prevent future problems and optimize performance on an ongoing basis by, for example, predicting the future resource allocation needs of workloads based on insights about how traffic patterns will change over time.
- **Measurement**: AIOps-driven analytics can also help organizations assess the effectiveness of their IT initiatives by providing continuous feedback loops across the software delivery lifecycle. How did a new application deployment impact performance and user engagement? How do business KPIs correlate with changes to the software environment? AIOps provides answers to questions like these on a continuous basis.

> In order to make a meaningfully positive impact on system performance and end-user experience, the analytics at the core of AIOps must produce actionable, tangible outcomes.

Dynamic Baselining

While understanding the concept of an anomaly is easy enough, what makes anomaly detection particularly challenging for AIOps in modern software environments is that, in many cases, there is no consistent means of defining "normal" operating conditions. The amount of network traffic, memory, and storage space that a given environment consumes might fluctuate widely throughout the day, for example. So could the number of active users or application instances.

Effective detection under these circumstances requires AIOps tools that are intelligent enough to set dynamic baselines. Dynamic baselines allow the tools to determine what constitutes normal activity under given circumstances (such as the time of day and the number of registered users for an application), then detect data or events that do not align with the dynamic baseline.

Drilling Down

The value of analytics within AIOps is not limited to understanding the state of systems as a whole. Just as important is the ability to drill down into a problem in order to investigate it at a deep level.

For example, if a web application is failing and you determine that the cause is network bandwidth limitations, you might want to be able to drill down and determine whether a certain type of network traffic—such as traffic from a specific region—was associated with the bottleneck that caused your application problem.

Insight such as this can help your ITOps team improve systems so that they are more resilient to the recurrence of problems. In this way, causal analysis with the assistance of AIOps not only helps to resolve problems in real time, but also helps to achieve continuous improvement by preventing problems from happening again.

Chapter 4: Implementing Intelligent Automation: From Insight to Action

In many cases, IT operations teams have employed limited automation that is based on custom-developed scripts or APIs that are connected to domain-specific tools. These approaches create islands of automation, which presents a challenge to handle cross-platform and cross-technology workflows.

That's why effective use of AIOps requires intelligent automation that can turn insight into action and reduce the toil that the IT team experiences when responding to incidents.

Automated Alarm Management

One way to do this is to ensure that alarm management is as automated and dynamic as possible.

Alerts that are configured manually to fire based on fixed thresholds do not work well in today's dynamic environments. Not only do manual alerts require considerable time to configure, but they can also lead to false positives because what constitutes acceptable risk, network or other resource consumption at one moment may change in the next moment, along with the environment. Instead of configuring manual alerting thresholds, AIOps tools can set thresholds automatically. They can also leverage dynamic baselining (discussed above) to configure when an alert should fire.

Alarm Context

Teams leveraging AIOps can also minimize toil and maximize actionability by ensuring that alerts come with all of the contextual information the team needs to respond to a problem.

Toward that end, rather than merely indicating that a problem has occurred, alerts should be accompanied by information that will help ITOps teams to respond to the problem. This means providing contextual information that will help engineers to understand a problem more thoroughly.

Actionable alerting can also include data-based resolution recommendations for engineers to consider. The ability of AIOps tools to provide recommendations, while leaving it to engineers to make the final determination about how to resolve a complex problem, is how AIOps enables true "intelligence": It empowers humans with AI-driven insights that allow them to act more quickly and decisively than they could hope to do using traditional remediation practices.

Leveraging Historical Data for Remediation

AIOps can also enable faster incident resolution and reduce toil by helping IT teams to interpret historical data associated with past issues in order to suggest solutions for similar incidents as they occur. Without AIOps, parsing through reams of logs and other data in order to identify the similarities between two incidents, and determine whether the resolution that worked for the first will also effectively address the second, is not feasible. AIOps-enabled solutions, however, can provide rapid insight based on historical data to help respond to this challenge.

Automated Resolution

As noted previously, AIOps tools can even take automatic action to resolve certain problems after they have identified them. They could block a host or close a port automatically in response to a security threat, for example, or spin up additional instances of an application if they determine that the existing instances are insufficient to meet demand.

Automated resolution is not practical in all situations; sometimes, the ultimate resolution to an incident will have to be implemented manually, even though AIOps can provide insights that help lead to the resolution. Yet, as machine-learning algorithms grow increasingly sophisticated, the problems that AIOps tools can resolve automatically will increase in number, enabling even faster and more seamless incident resolution.

Automated Ticket Management

A typical IT organization may receive anywhere from dozens to hundreds of support tickets per day. Those tickets cost, on average, $1.60 per minute to address—a figure that quickly adds up when the IT team relies on manual, time-consuming ticket resolution.[5]

AIOps addresses this challenge by enabling a highly automated approach to ticket management. AIOps tools can automatically prioritize tickets so that IT teams know which ones to focus on. They can also help engineers find the root cause of a reported issue in order to resolve it more quickly. And in some cases, AIOps solutions can apply automated resolutions to close tickets on their own, without consuming IT engineers' time at all.

In this way, AIOps not only reduces the cost of ticket management, but also significantly accelerates response to incidents, leading to happier users and better business outcomes.

Chapter 5: Tips to Adopting an AIOps Solution

AIOps is a transformative technology, but leveraging it does not require a total transformation of your business' IT strategy. AIOps can be implemented incrementally, by building on existing investments in processes and tools, rather than rebuilding everything from the ground up.

Let's look at how to go about adopting an AIOps solution.

Define Your Goals

The first step in AIOps adoption is to make clear the outcome your business hopes to achieve by implementing AIOps: Moving from an IT operating model that is based on manual workflows to one that is as close to hands-off as possible.

Identifying this goal, and getting buy-in for it from all stakeholders (including business leaders as well as members of the IT organization), is important for ensuring that AIOps adoption doesn't become another technological change you make just for the sake of making a change, without a clear goal in mind. Just as you shouldn't move to the cloud without first identifying the key goals you want to achieve from the cloud, you shouldn't begin your AIOps adoption process until you know which concrete effects the change will have on your business.

[5] HDI, "**Metric of the Month: Service Desk Cost per Ticket**," Jeff Rumburg, May 2, 2017

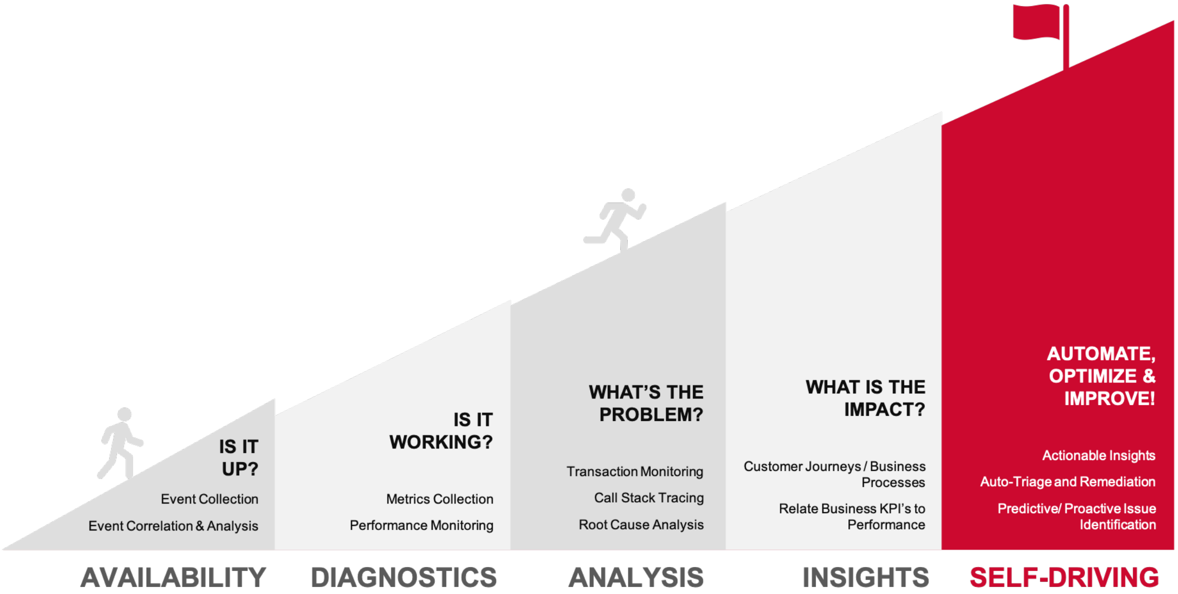

Figure A. The move to adopt AIOps is a journey, rather than a single, point-in-time event.

AIOps is a Journey

AIOps adoption becomes even more seamless when you recognize that AIOps is a journey, not something you implement overnight.

For most teams, AIOps implementation starts with evolving existing monitoring practices to bring organizations closer to achieving the full effect of AIOps. If today you are monitoring systems just to detect problems, for example, you can take your first steps toward AIOps by focusing on adding contextual information to your alerts so that you don't just detect issues but also help remediate them. Or, if your data sources are highly siloed today, move toward AIOps by integrating and correlating them to provide deeper visibility.

Remember, too, that you don't need to apply AIOps to your entire IT estate in one go. Most teams start small by deploying AIOps to address select use cases or certain data sources. For example, you might leverage AIOps to help manage a particular microservices-based application that is difficult to observe and troubleshoot using conventional monitoring tools. From there, you can scale up your AIOps practices to address other applications as well.

Your AIOps use cases can evolve over time, too. It's common to start with basic root-cause analysis and normalization, then move onto automated remediation; and finally, to predictive analytics. The extent to which AIOps tools integrate with other IT processes, and to which you customize your AIOps tools and practices, will also naturally evolve along with the complexity of your AIOps use cases.

Engage a Trusted Partner

Any monitoring tool can be labeled an AIOps solution. But not all monitoring tools deliver the automated analytics, intelligence, and actionable insights that enable fully functional AIOps.

That's why it's important to select an AIOps platform and vendor with deep experience in this growing frontier of the IT industry. Broadcom has not only been offering an AIOps solution to customers for years, but has also invested heavily in AIOps practices to help manage its own IT environments. As a trusted partner with extensive domain expertise in AIOps, Broadcom is uniquely positioned to help other businesses make the leap from conventional monitoring to AIOps.

Chapter 6: The Future of AIOps

Although AIOps is a mature solution that already forms a core part of the IT strategies for many businesses, it remains a dynamic and fast-evolving segment of the IT industry.

Going forward, expect AIOps to become even more valuable, thanks to the following trends.

Domain-Centric vs. Domain-Agnostic AIOps

Gartner divides the AIOps market into two key segments. One is composed of so-called domain-centric AIOps tools, which focus on particular use cases, like application performance monitoring. The second is domain-agnostic AIOps tools that can be deployed broadly for any type of IT need, and that can support multiple use cases at once.

While domain-centric tools, which are easier to implement, have been the most common type of AIOps solution to date, the most sophisticated solutions in the future will likely focus on delivering domain-agnostic AIOps that can cater to any and all IT needs. At the same time, however, advanced AIOps vendors will continue to offer domain-centric AIOps tools that focus on addressing complex and specialized use cases. Broadcom's AIOps solution can address both types of scenarios, depending on business needs.

Better Business Outcomes

AIOps is poised to play an increasingly important role in ensuring that the practices of technical teams align with and reinforce business goals.

For example, according to Gartner, by 2025 75 percent of product and platform teams will leverage AIOps for automated change risk analysis within DevOps pipelines in order to reduce unplanned downtime.[6] In this way, AIOps will help ensure that fast-moving DevOps teams are able to identify and act upon key business priorities, rather than simply performing DevOps processes for their own sake without measuring their impact on the business.

Put another way, AIOps is rapidly becoming an integral part of the software development lifecycle by driving stronger integration between technical stakeholders and business stakeholders.

Security Analytics

Helping IT teams to remediate issues faster while reducing toil was the primary focus on AIOps, and it is likely to remain so for the foreseeable future.

However, security analytics are becoming an increasingly important secondary area of focus for AIOps tools. Identifying, analyzing, and responding to security threats is growing only more challenging as IT environments become more complex, and as threat actors leverage ever-more creative ways to breach environments.

By helping security analysts to interpret threats, and in some cases to respond to them automatically, AIOps will help security teams remediate vulnerabilities faster and more efficiently, just as it does for IT problems. In turn, AIOps allows teams to bridge the gap between security and IT operations by enabling both groups to work better together, implementing the practices associated with DevSecOps.

[6] Gartner, "**Platform Teams and AIOps Will Redefine DevOps Approaches by 2025**," January 6, 2021, ID: G00732214, Analysts: George Spafford, Manjunath Bhat

Get Started with AIOps

Broadcom has been at the forefront of the AIOps ecosystem since its introduction several years ago, and will continue to lead the way as AIOps evolves.

Today, Broadcom offers an AIOps solution through **DX Operational Intelligence**. DX Operational Intelligence is an AIOps platform that leverages data from diverse sources—ranging from the cloud, to on-premises, to the mainframe—to enable full-stack observability, fully automated analysis, and autonomous remediation. The result is lower MTTR, higher availability, optimized performance, and minimal toil on the part of IT teams.

To learn more about how Broadcom can help your business begin its AIOps journey, and view stories detailing how organizations have already benefited from AIOps, visit our **AIOps resource hub**.

About Broadcom
Broadcom Inc. (NASDAQ: AVGO) is a global technology leader that designs, develops and supplies a broad range of semiconductor and infrastructure software solutions. Broadcom's category-leading product portfolio serves critical markets including data center, networking, enterprise software, broadband, wireless, storage and industrial. Our solutions include data center networking and storage, enterprise and mainframe software focused on automation, monitoring and security, smartphone components, telecoms and factory automation. For more information, go to www.broadcom.com.

ca® technologies
A Broadcom Company

The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com. Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.