AIOps

Artificial intelligence for IT operations, or AIOps, is the application of artificial intelligence (AI) capabilities—such as natural language processing and machine learning models—to automate, streamline and optimize IT service management and operational workflows.

AIOps leverages big data, analytics and ML capabilities to:

- Ingest and aggregate the huge (and ever-increasing) volumes of data generated by IT components, application demands and performance monitoring tools and service ticketing systems in an enterprise tech stack.

- Intelligently shift signals out of the "noise" to identify significant events and patterns related to application performance and availability issues.

- Diagnose root causes and report them to IT and DevOps for rapid incident response and remediation or, sometimes, automatically resolve these issues without human intervention.

By integrating separate manual IT operations tools into a single intelligent, automated IT operations (ITOps) platform, AIOps enables IT operations teams to respond quickly—and often proactively—to slowdowns and outages, with end-to-end visibility and context.

It helps businesses bridge the gap between diverse, dynamic and difficult-to-monitor IT landscapes and siloed IT teams on one hand and user expectations of app performance and availability on the other. With the proliferation digital transformation initiatives across business sectors, many experts see AIOps as the future of IT operations management.

AIOps components

AIOps can incorporate a range of AI strategies and features, including data output and aggregation, algorithms, orchestration and visualization.

Algorithms codify IT expertise, business logic and goals, enabling AIOps platforms to prioritize security events and make performance decisions. Algorithms form the basis for machine learning (ML) and enable platforms to establish baselines and adapt as environmental data changes.

Machine learning uses algorithms and techniques—such as supervised, unsupervised, reinforcement and deep learning—to help systems learn from large datasets and adapt to new information. In AIOps, ML helps with anomaly detection, root cause analysis (RCA), event correlation and predictive analysis.

AIOps programs gather data from various network components and data sources. **Analytics** interpret the raw data to create new data and metadata that helps both systems and teams identify trends, isolate problems, predict capacity demands and manage events.

Automation features within AIOps tools enable AIOps systems to act based on real-time insights. For example, predictive analytics may anticipate an increase in data traffic and trigger an automation workflow to allocate additional storage as needed (in keeping with algorithmic rules).

Data visualization tools in AIOps present data through dashboards, reports and graphics, so that IT teams can monitor changes and make decisions beyond the capabilities of AIOps software.

How does AIOps work?

AIOps uses a big data platform to aggregate siloed ITOps data, teams and tools in one place. This data can include:

- Historical performance and event data

- Real-time operations events

- System logs and metrics

- Network data, including packet data

- Incident-related data and ticketing

- Application demand data

- Infrastructure data

AIOps platforms then apply focused analytics and ML tools to:

- **Separate significant event alerts from the "noise."** AIOps combs through ITOps data and separates signals, differentiating abnormal events from noise (everything else) and identifying data patterns.

- **Identify root causes and propose solutions.** AIOps can correlate abnormal events with other event data across environments to zero in on the cause of an outage or performance problem and suggest remedies.

- **Automate responses, including proactive, real-time resolution.** At a minimum, AIOps tools can automatically route alerts and recommended solutions to the appropriate IT teams and even create response teams based on the nature of the problem and the solution. In many cases, they can also process ML results and trigger automatic system responses to address problems as they emerge (and often, before users know they occurred).

- **Learn continually, to improve handling of future problems.** AI models can help systems understand and adapt to changes in the environment (when a DevOps team provisions new infrastructure or reconfigures existing infrastructure, for instance).

Implementing AIOps

The journey to AIOps is different in every organization. Once business leaders distill an AIOps strategy, they can start to incorporate tools that help IT teams observe, predict and respond quickly to IT issues.

When choosing tools to improve AIOps, many teams consider the following features:

- **Observability:** Observability is the extent to which you can understand the internal state or condition of a complex system based only on knowledge of its external outputs. The more observable a system, the quicker and more accurately teams can navigate the path from identified performance problems to root causes, all without additional testing or coding.

  Leading observability tools provide deep visibility into modern distributed business services and applications for faster, automated problem identification and resolution.

  In IT and cloud computing, observability uses advanced software tools and practices to aggregate, correlate and analyze steady streams of performance data from distributed applications—and the hardware and networks they run on. Observability facilities more effective app and network monitoring, troubleshooting and debugging processes so that systems continue to meet user experience expectations, service level agreements (SLAs) and other business requirements.

- **Predictive analytics:** Predictive analytics is a branch of advanced analytics that makes predictions about future outcomes using historical data, statistical modeling, data mining techniques and machine learning. In AIOps, teams use predictive analytics to find data patterns and identify risks and opportunities.

  Modern enterprises are inundated with data from disparate data repositories across the organization. Predictive analytics uses tools such as logistic and linear regression models, neural networks and decision trees to gain actionable insights from massive quantities of enterprise data and make predictions about future system events.

- **Proactive response:** Some AIOps solutions proactively respond to unintended events (such as slowdowns and outages), bringing application performance and resource management together in real time.

  By feeding application performance metrics into predictive algorithms, teams can identify patterns and trends that coincide with different IT issues. And given their ability to forecast IT problems before they occur, AIOps tools can automate resolution to address system issues promptly.

Incident response automation technologies are integral to effective IT systems management. They can help businesses improve both the client and customer experience and significantly improve key performance metrics, such as mean time to detection (MTTD). Furthermore, AIOps systems provide a safety net for IT operations teams, addressing issues that might fall through the cracks with only human oversight.

Comparing domain-agnostic and domain-centric AIOps tools

AIOps platforms can provide organizations varying levels of automation, depending on their IT needs and AIOps strategy.

With a domain-agnostic approach, AIOPs software collects data from a wide range of sources to solve problems across various operational domains (networking, storage and security, for example). These tools offer a comprehensive, holistic view of overall performance, helping organizations address issues that span multiple areas.

However, they might not provide the detailed insights IT teams need to tackle specific pain points or cater to unique industry needs. The broad nature of domain-agnostic tools means they excel in offering a general overview, but they might fall short in delivering targeted incident management solutions for nuanced challenges.

Domain-centric AIOps tools focus on a specific domain, whether it's an IT environment or a particular industry. Though these tools don't cover the entire IT landscape, they are highly specialized, with AI models trained on datasets specific to their domain. This specialization enables them to provide precise insights and solutions.

For instance, in a network context, a domain-centric tool can accurately identify the cause of a bottleneck by understanding standard network protocols and patterns. And thanks to its specialized training and focus, it can determine whether the slowdown is the result of a distributed denial-of-service (DDoS) attack or a simple system misconfiguration.

Regardless of the type of tool an organization chooses, it's important that teams:

- Train AI models using comprehensive, representative datasets for optimal reliability and accuracy.

- Use transparent, fair AI models so that stakeholders can understand AI-based decision-making.

- Train IT teams to use tools and insights effectively for a smoother AIOps transition.

- Assign a human being to oversee and validate the AI model's conclusion to keep teams and systems accountable.

AIOps vs. DevOps

Both AIOps and DevOps are methodologies designed to enhance IT operations, but they focus on different aspects of the software lifecycle.

DevOps aims to integrate development and operations teams to foster collaboration and efficiency throughout the software development process. It streamlines and automates coding, testing and deployment processes and accelerates continuous integration and continuous delivery (CI/CD) pipelines, enabling faster, more reliable software releases.

DevOps also uses tools such as infrastructure as code and collaboration platforms to break down silos between teams and make sure that software updates can be delivered quickly, without compromising quality.

Whereas DevOps focuses on accelerating and refining software development and deployment, AIOps uses AI to optimize the performance of enterprise IT environments, ensuring systems run smoothly and efficiently. AIOps platforms use ML and big data analytics to analyze vast amounts of operational data to help IT teams to detect and address issues proactively.

When used in tandem, AIOps and DevOps services can help business create a complementary, comprehensive approach to managing the entire software lifecycle.

AIOps use cases

AIOps services can help businesses tackle several use cases, including:

Root cause analysis

Root cause analyses (RCAs) determine the root cause of problems to remediate them with appropriate solutions. RCA helps teams avoid the counterproductive work of treating symptoms of an issue, instead of the core problem.

For example, an AIOps platform can trace the source of a network outage to resolve it immediately and set up safeguards to prevent the same problem from occurring in the future.

Anomaly detection

AIOps tools can comb through large amounts of historical data and discover atypical data points within a dataset. These outliers help teams identify and predict problematic events (data breaches, for instance) and avoid the potentially costly consequences of those events (negative PR, regulatory fines and declines in consumer confidence, among other issues).

Performance monitoring

Modern applications are often separated by multiple layers of abstraction, making it difficult to understand which underlying on-premises servers, storage resources and networking resources are supporting which applications. AIOps helps to bridge this gap.

It acts as a monitoring tool for cloud infrastructure, virtualization and storage systems, reporting on metrics including usage, availability and response times. Furthermore, AIOps uses event correlation capabilities to consolidate and aggregate information so that users can consume and understand information more easily.

Cloud adoption and migration

For most organizations, cloud adoption is gradual, not wholesale. This often results in hybrid [multicloud environment](#)s (including many interconnected parts that rely on technologies such as [APIs](#) and [microservices](#)) with multiple dependencies that can change too quickly and frequently to document. By providing clear visibility into these interdependencies, AIOps can dramatically reduce the operational risks associated with [cloud migration](#) and [hybrid cloud](#) approaches.

DevOps adoption

DevOps speeds development by giving development teams more power to provision and reconfigure [IT infrastructure](#), but teams still must manage the architecture. AIOps provides the visibility and automation IT teams needs to support DevOps without excessive human oversight.

Benefits of AIOps

The primary benefit of AIOps is that it enables ITOps teams to identify, address and resolve slowdowns and outages faster than they could by manually sifting through alerts from multiple tools and components. This enables businesses to achieve:

Faster mean time to repair (MTTR)

By cutting through IT operations noise and correlating operations data from multiple IT environments, AIOps can identify root causes and propose solutions faster and more accurately than humanly possible. Accelerated problem identification and incident resolution processes enable organizations to set and achieve previously unthinkable [MTTR](#) goals.

Lower operational costs

Automatic identification of operational issues and reprogrammed response scripts reduce operational costs and drive more precise resource allocation. It also reduces IT staff workloads and frees up staffing resources for more innovative and complex work, improving the employee experience.

Better observability and collaboration

Integrations within AIOps monitoring tools facilitate more effective collaboration across DevOps, ITOps, [governance](#) and security teams. And better visibility, communication and transparency enable these teams to improve decision-making and respond to issues faster.

Predictive ITOPs management

With built-in predictive analytics capabilities, AIOps platforms continuously learn to identify and prioritize the most urgent alert. This helps IT teams address potential problems before they lead to unplanned downtime, disruptions and service outages.