



AIOps:

The journey from reactive to proactive ITOM for modern IT infrastructures

Sharon A Ratna, Product consultant

Executive summary

Modern IT infrastructures are reinventing rapidly and pivoting to intelligent, automated, and autonomous network management processes. AIOps platforms have introduced a paradigm shift in how ITOM is traditionally perceived. With each new day, a new announcement of a better and more intelligent AIOps solution rocks the market. However, with organizations under tight budget constraints after years of enduring the pandemic and now a slow economy, implementing an AIOps solution requires a critical requirement fit-gap analysis, strong proof of ROI, and delivery of desired business process optimizations and outcomes.

With a projected market size of about \$2.1 billion in 2025, and a compound annual growth rate (CAGR) of around 19%^[a], the expectation for AIOps adoption is high. But is the hype realistic, or is it just a fad?

In this whitepaper, we discuss the factors that have driven the industry's hype around AIOps. Starting with AIOps' five defining capabilities and the difference made by AI-enriched ITOM, we will be examining the effective implementation of AIOps in your IT infrastructure and understand its maturity stages and potential business impact. We will also be discussing the past, present, and future of AIOps offerings and the market alongside the current challenges.

Index

1. Overview: What is AIOps?
2. Understanding AIOps: The 5 defining capabilities
 - Cross domain data ingestion
 - Asset relation topology
 - Event correlation and incident inspection
 - Pattern recognition
 - Remediation
3. AI enriched ITOM: What is the AIOps difference and why should you care?
 - Probabilistic root cause analysis
 - Event noise filtering
 - Intelligent incident management, automation and remediation
 - Cost optimization with unified proactive monitoring
 - DevOps, ITOM, and the power of AI
4. Implementing AIOps: Transforming from a manually reactive to a data-driven, proactive operational state
 - The build vs. buy conundrum: 10 factors to consider
 - DIY AIOps foundational requirements and abstract architecture
 - AIOps implementation maturity and business impact model
 - Implementation challenges
5. AIOps: The past, present, and future
 - AIOps market: The hype cycle and market growth over the years
 - A glimpse of the future: What to expect?
6. Glossary of terms
7. References

Chapter 1: Introduction to AIOps

Overview: What is AIOps

Innovation has always been at the core of decades of efforts toward optimizing ITOM processes and costs. Diverse monitoring tools that offer end-to-end network monitoring, instant alerts, and threshold-based configurations to detect network anomalies have simplified ITOM for enterprises. However, the increased change velocity, impact of disruptive technological innovations, and organizations' shift towards digital transformation are laying a strain on the conventional reactive capabilities of disparate network monitoring siloes deployed.

Unifying the ITOM siloes is now possible with the advent of AI-enriched ITOM i.e., AIOps. AIOps drive intelligent data-based decision-making in modern IT infrastructures. With its capabilities to apply machine learning combined with big data analytical models, AIOps offers proactive performance monitoring, pattern recognition, event correlation, prediction, and enhanced incident management.

As defined by [Gartner](#),

AIOps combines big data and machine learning to automate IT operations processes, including event correlation, anomaly detection, and causality determination.

Currently, at its peak of inflated expectations among the IT community and a predicted AIOps service usage rise from 5% in 2018 to 30% in 2023[a], AIOps is experiencing meteoric adoption rates in modern IT infrastructures. With demonstrated expeditious return on investments and optimized business operation processes, the adoption growth accelerators of AIOps include,

- **IT data deluge:** Making sense of the cornucopia influx of network metrics and monitoring data from monitoring solutions deployed.
- **The burgeoning tool sprawl:** Siloed disparate sources of truth as a result of efforts to achieve full-stack network visibility.
- **Alert fatigue:** Need to differentiate signals from event noise.
- **Increasing expectations:** Need for faster infrastructure-issue resolutions and service availability including ensuring reduced mean time to discovery (MTTD), mean time to repair (MTTR), high mean time between failures (MTBF), and mean time to failure (MTTF).
- Need for better data-driven decision-making
- Predicting issues before they disrupt the network functionality
- Supporting increased network change velocities and offer enhanced agility
- Autonomous incident mitigation and remediation
- Cost saving and resource utilization efficiencies.

Chapter 2: How does AIOps work

Understanding AIOps: The 5 defining functionalities

AIOps platforms offer enhanced data analysis, event noise filtering, and automated mitigation enabled by the following five capabilities:

- Cross domain data ingestion
- Asset relation topology
- Event correlation and incident inspection
- Pattern recognition
- Remediation

Cross domain data ingestion

Data forms the basis of AIOps functionalities. The AIOps platform leverages a wide array of data including the network's sensory and event data across domains. Data is an important inflow that the AIOps engine analyzes, identifies patterns, establishes correlations, and carries out intelligent actions as required, on.

The AIOps platform can only be as good as the data ingested making cross domain data collection a fundamental aspect. This requires organizations to first ensure the deployment of reliable data collection, management, and governance methods and mechanisms.

In modern IT infrastructures,

Implementing advanced data fabrics or meshes offers enhanced data access, governance, federation, and interoperability across distributed teams and systems. The data inflow from these meshes when fed to the AIOps platform enables much more precise and critical data supply from the entire organizational processes when compared to traditional data lakes and warehouses.

Post data collection and ingestion, the AIOps platform runs data analysis leveraging its big data capabilities. The collected data is indexed, normalized, and analyzed as and when streamed. ML capabilities are further used for real-time stream data analysis and historical data analysis.

Asset relation topology

AIOps platforms are capable of automated discovery and dependency mapping (DDM) by analyzing their ingested data feed. By deciphering the asset relationship between different components including business services, servers, containers, load balancers, and databases from implicit and explicit sources, the AIOps platform internally builds asset relations.

Visibility into the physical and logical relationships of discrete network nodes and links enhances the AIOps platform capabilities including root cause analysis. Topology in causality chain identification can provide the platform with accurate tracking and topographic correlation building. The asset relation and dependency across multiple networks and business layers are correlated and visualized by the platforms' intelligent dependency mapping capabilities.

In modern IT infrastructures,

that are cloud heavy are required to closely monitor their ephemeral Infrastructure as Code (IaC) and systems since these infrastructures and their asset relations are subjected to frequent changes. For AIOps platform to sense these changes and intelligently modify or create its internal asset relations, real-time topology and telemetry data needs to be continually ingested. This again reiterates that the AIOps platform can only be as good as the data ingested.

Event correlation and incident inspection

Amid the deluge of telemetry, event alarms, and business processes data ingested into the AIOps platform, the platform is capable of detecting meaningful patterns. Intelligent event noise filtering is enabled by effective event data entropy configurations. With this, the AIOps platform filters, unduplicates, and normalizes the event data to find relationships and identify causation.

The AIOps platform analyzes the event data ingested and asset relation topology to build different correlations including,

- **Topology-based correlation:** This identifies the causation of an event based on the physical and logical topology of the affected node and its connected links.
- **Event co-occurrence correlation:** The platform identifies the event causality based on the time proximity and the sequence of event occurrence.
- **History-based correlation:** The platform compares the newly identified events to historically redundant or related events and event code books of different domains to identify the nature and causation of an event.

In modern IT infrastructures,

topology-based event correlation helps effectively identify event causation across business domains with ease. Let's say, an organization's human resources department is facing slower payslip processing time. The AIOps platform with sufficient data input can correlate event data to identify the cause to be the slower loading speed of a payment processing application running on the finance team's servers. Thus offering cross domain topology based correlations.

Pattern recognition

The AIOps platform analyzes rich data sets and event metrics that aid in detecting patterns that indicate critical anomalies in real time. By analyzing patterns formed by multiple metrics, AIOps platforms employ Multivariate Anomaly Detection to offer enhanced incident management by identifying leading indicators and the root cause of the event causality. The rich domain expertise established by statistically supervised learning models and probabilistic ML models enables automated pattern discovery, anomaly detection, and causality determination along with adaptive prescriptive analysis.

According to our recent survey.

***28%** of IT admins find correlation of device data to understand patterns and resolve issues to be challenging when it comes to pursuing a modern, adaptive, and fast paced operating environment.*

The ML component of the AIOps platform analysis historical data and event logs to identify historical baselines. These baselines became a part of the model training set that further ensure continual learning and AIOps platform improvement. This enhances the platform's intelligent capabilities to learn and recognize more complex patterns.

Remediation

AIOps platforms continually improve their capabilities through observed operational response-based learnings and explicit operator specifications. It continually improves the event identification, prediction, and remediation capabilities through supervised, unsupervised, and fuzzy match learning. This, in turn, helps the platform improve its event identification, pattern matching, and incident correlation capabilities.

The AIOps platform makes recommendations based on the detected and predicted events which are then communicated with an external system. The effectiveness of the AIOps platform's automation and remediation capabilities is realized by its integration with external orchestration systems such as runbook and alerting and ticketing platforms. Intelligent remediation and alerting automated by the AIOps platform are relied upon by the network engineers and SREs through these integrations.

Chapter 3: Experiencing the AIOps difference in ITOM

AI-enriched ITOM: The AIOps difference and why you should care

With digital transformation now becoming a core part of an organization's processes, expecting modern IT infrastructures to be run with traditional siloed monitoring solutions is impractical. Monitoring rapidly changing IT infrastructures requires making sense of the data deluge, detecting disruptive events, event causality, intelligent alerting, and automated remediation.

Modern IT infrastructures can meet these requirements with the AIOps platforms' promise of unifying operational siloes, enhanced data analytics, root cause analysis contextualization, and autonomous operations. An investment in the AI and automation capabilities to enhance ITOM delivers ROI in the form of tangible business values and ITOM process efficiencies including:

- Probabilistic root cause analysis
- Event noise filtering
- Intelligent incident management, automation, and remediation
- OpEx optimization with unified proactive monitoring
- DevOps, ITOM, and the AIOps advantage

Probabilistic root cause analysis

The AIOps' capability to identify event causality and offer probabilistic root cause analysis significantly reduces the time taken for IT engineers and SREs to identify and determine the problem statement of a

network issue. The considerable improvements in the mean time to detect are further boosted by the AIOps platform's root cause analysis contextualization capability.

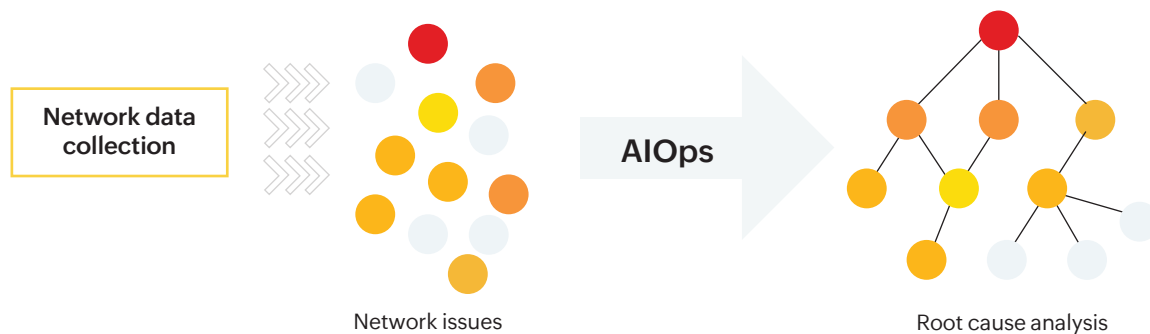


Fig 3.a, Probabilistic root cause analysis with AIOps

AIOps platforms analyze a myriad of sensory and event data along with topology to cut through all the infrastructure layers. This helps ensure the root cause can be identified, and the resulting network, business, and end-user impacts can be analyzed.

According to a recent survey,

*Around 44% of mid-sized and large enterprises indicate that hourly downtime costs range from **\$1 million to over \$5 million**, exclusive of any legal fees, fines, or penalties. The hourly cost of downtime now exceeds \$300,000 for 91% of small and medium enterprises, and large enterprises[c].*

Creating an actionable context around the network event helps organizations rapidly troubleshoot critical issues and enable quicker service restoration. This significantly reduces MTTR and downtime costs.

With the newly identified probabilistic root cause analyses and based on the observed external response and automation techniques applied, the AIOps platform can analyze, learn, and build better correlations and incident, prediction models. This proactive and continually evolving root cause analysis capability offered by AIOps enables organizations to view real-time network threats, stop cascading network issues from disrupting preferred network functionality, and minimize costs.

Event noise filtering

According to a recent survey,

*In security domain, nearly **45%** of all alerts are false positives. These false positives can cause the same amount of downtime as actual alerts[b].*

With traditional siloed ITOM solutions, data accuracy and alert significance can be hard to establish given the unfiltered inflow of considerable event data in tandem with event noise.

In modern IT infrastructures,

A problematic server can affect 100 end users at the same time, causing 100 new user experience alerts and one server performance alert to be raised. While the issue is just in one server, the related IT teams including I&O, end user and applications management teams are loaded with a storm of end user alerts.

As stated above, events with domino effects can easily create increased alert noise in the event data received. Filtering the signal from the noise is important to ensure no critical alert goes

undeducted and that IT teams are not overloaded with tackling copious insignificant alert scenarios.

To enable noise reduction, the AIOps platform deploys several effective noise entropy models and correlation techniques to map the alert generated to its business impact. Based on the scale of impact, the AIOps platform assigns alert priority and displays all the critical alerts in a single pane of alert view.

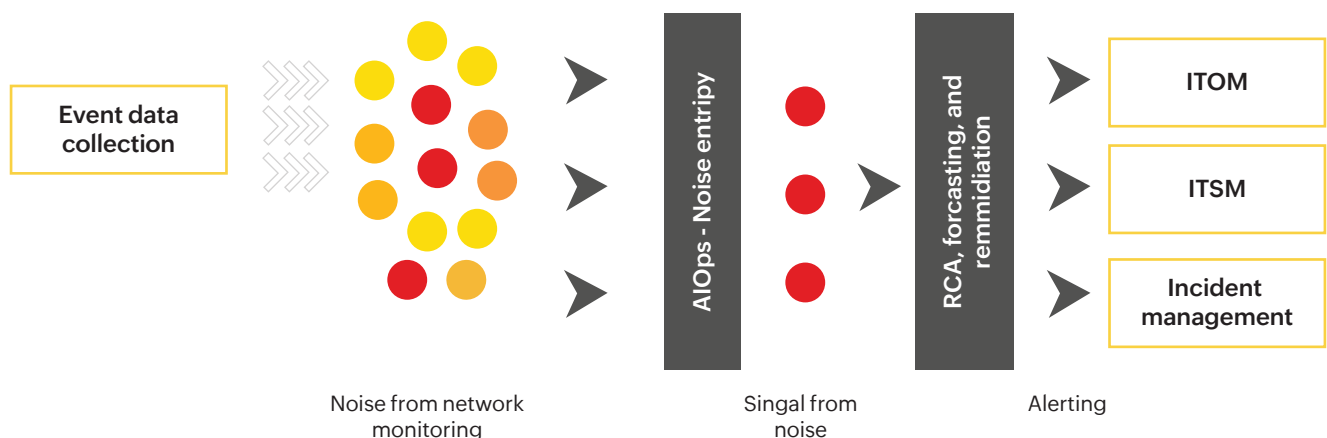


Fig 3.b, Event noise filtering with AIOps

This reduces alert fatigue for IT engineers and SREs, significantly improves the mean time to detect, and ensures that no critical event is concealed.

Intelligent incident management, automation, and remediation

Modern IT infrastructures need to be one step ahead of emerging network issues to ensure uninterrupted network availability.

The IT teams need to pedal exponentially faster to keep up with the network changes and detect and tackle cascading network issues from resulting in a full-blown network outage. Network outage incidents are no longer a rarity in modern IT infrastructures. This has made the need to detect, resolve, and prevent these outages critical.

Before AIOps, this required data collection, incident detection, and the incident being analyzed by the ITOM team for the level of impact and affected devices, alongside ITSM teams drowning in tickets.

50%

Large enterprises experience loss due to network outages(4)

60%

of failures cost at least **100,000** in total losses. (5)

1 in 5

organizations reported "severe" or "serious" downtime in last 3 years (5)

AIOps is changing this paradigm to a more intelligent, automated, and intuitive process with minimal need for human interaction. Capable of processing complex anomalies and inherent threat detection, AIOps platforms easily identify changes in network behavior.

In IT infrastructures,

For instance, a traditional ITOM solution monitoring CPU utilization offers alerts such as "CPU utilization has reached 90%".

Whereas, an AIOps solution correlates the current CPU utilization metrics with learned and historical patterns to offer alerts such as "CPU utilization will reach 90% in 2 days."

This offers a proactive approach to averting issues and monitoring critical network components.

The capability of "finding a solution before the problem occurs" is further enhanced by the AIOps platform's automated remediation capability. At its current stages, not many AIOps platforms are fully autonomous. However, with the aid of rules-based automation (RBA), scripts, orchestration tools, and human-in-the-loop (HITL) automation processes, AIOps platforms enable semi-autonomous automation and remediation. The actionable intelligence offered by the AIOps platform is translated into proactive and cohesive incident mitigation, operations monitoring, and management processes.

Cost optimization with unified proactive monitoring

The CapEx of installing, integrating, and adopting AIOps platforms can be debatable when organizations

are running under a tight budget constraint given the current scenario. However, the jeopardizing effect of downtime and brownouts on an organization's budget makes a compelling case for implementing AIOps. No organization is fully immune to network outages in spite of its state-of-the-art IT infrastructure and best-of-breed monitoring tools. Over the years, even the biggest tech giants have fallen prey to network outages.

Meta

Downtime (1)
Oct - 2021
Loss: **100 Million**
Cause: Faulty configuration

Amazon

AWS outage (2)
March 2017
Loss: **150 Million**
Cause: Human error

Apple

AppStore outage(3)
March 2015
Loss: **17 Million**
Cause: DNS error

A common factor in all these outages that has had an enormous effect on the organization's yearly budget is the time taken to bring the network or services back online. Every second counts. Especially if your organization depends heavily on its IT infrastructure for its core business functions.

The longer the MTTK, MTTD, and MTTR, the higher the costs—both tangible and intangible including reputation loss and degraded customer experience.

With its benefits, ROI, and OpEx optimization outweighing its initial CapEx, investing in AIOps is a compelling argument organizations should consider.

According to a recent survey,

*Deploying AIOps solutions has enabled **26%** reduction in percentage of IT budgets spent on operating and maintaining IT services.*

53% of organizations are creating cost efficiencies across domains[d].

62% of companies see “very high” or “high ROI” from their AIOps investments[i].

Few of the OpEx optimization opportunities made possible by AIOps includes,

- Business service reliability and performance reduce the hefty losses due to downtime and service unavailability.
- With shortened MTTD and MTTR, AIOps significantly reduces the issue rectification costs that lay a strain on the ITOM budget.

- The reduced need for human interaction and manual tasks implies the reduced need for staff. With monotonous tasks now automated, AIOps enable IT teams with more time to focus on other tasks.
- Continuous learning mechanisms assure continued process optimizations. Also, with the learning loop also including human–IT interaction observation-based learning, the AIOps platform can effectively carry out more tasks that previously required human involvement.
- The cross-domain awareness enabled by the AIOps platform enables unified ITOM offering time and resource optimization.
- With AIOps offering built-in AI and ML models and big data analysis capabilities, it offers easier adoption, and organizations require lesser investment in staff training.
- The prediction and forecasting capabilities of AIOps help enhance capacity planning with required cost optimizations.

*In our **2022 IT digital dominance survey**, 21% of the respondent organizations told us that they were looking to implement AIOps tools for its predictive analysis capabilities.*

DevOps, ITOM, and the AIOps advantage

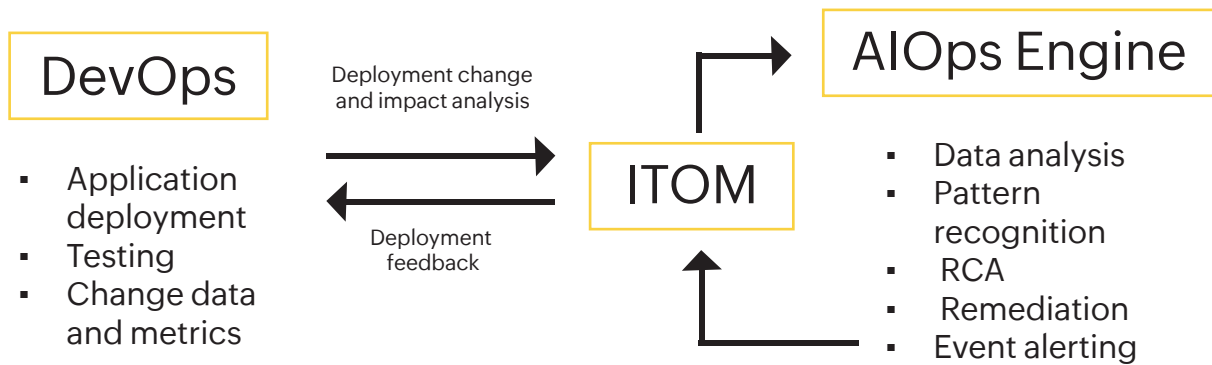
Modern IT infrastructures are growing increasingly reliant on DevOps practices to improve application quality and deployment efficiently through agile, lean, and collaborative approaches. Offering fast-paced application development, deployment, monitoring, and enhancement, the effectiveness of DevOps also depends on the ITOM capabilities at its disposal.

ITOM offers the fundamental foundations for DevOps teams to gain insights into the deployment impact and network change analysis.

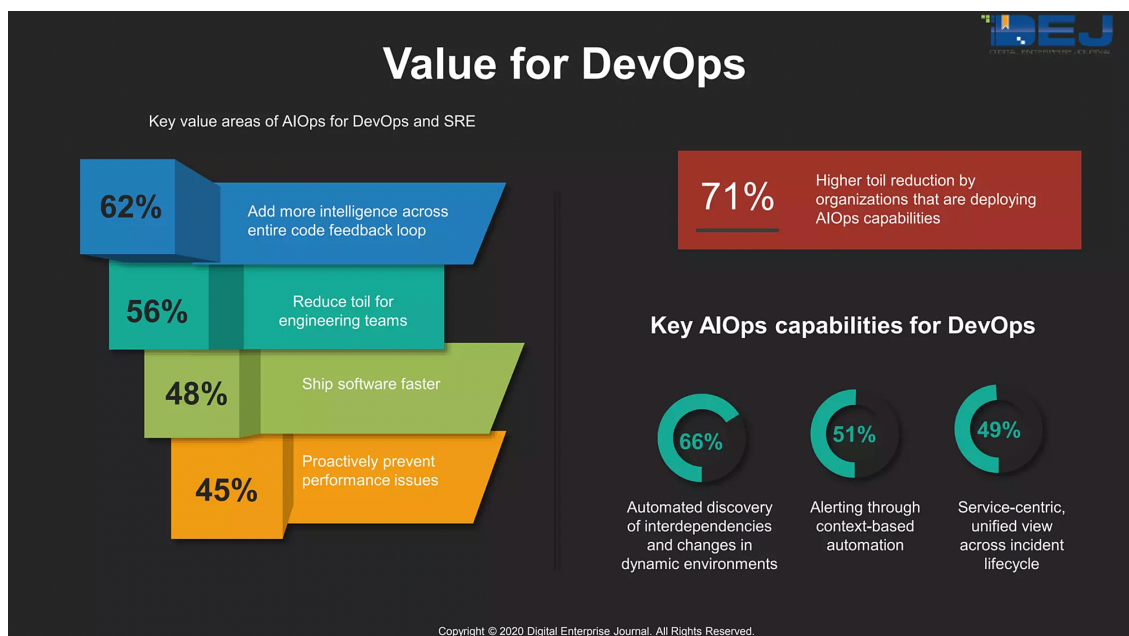
In modern IT infrastructures,

When DevOps teams are testing deployments in IT infrastructures, it can cause a series of configuration changes across the network components. If any deployment triggers a configuration failure or resource overutilization, without proper tracking of the network performance metrics, configurations, and event and telemetry data, the issue can go undetected. This eventually leads to deployment failure. The faster the changes, the more difficult it becomes to track without the right capabilities.

This is where AI-enriched ITOM capabilities help DevOps teams to forecast, identify, and resolve incidents before they cripple the deployment. Most incidents are often presaged by a specific order of events. AIOps identifies and analyzes this order to alert the DevOps team to mitigate the issue before the incident takes place.



This reduces deployment impact analysis complexity and enhances productivity with integrated workflow automation and continuous improvements.



Chapter 4: Implementing AIOps in your organization

Implementing AIOps: Transforming from a manually reactive to a data-driven, proactive operational state

"There is no time like the present" is probably the best-suited answer to the **"when should we try out AIOps?"** debate in organizations that are yet to test the waters. The urgency to implement is rather what the industry demands than suggests. Along with the benefits discussed above, the need to stay ahead of the competition, relevant to the market, and in trend with the newer technological developments such as hybrid networking and distributed systems, has fueled organizations to consider AIOps implementation opportunities at the earliest.

Here's a glimpse of sentiments around AIOps implementation,

"Become familiar with AI and ML vocabulary and capabilities today, even if an AIOps project isn't imminent. Priorities and capabilities change, so you may need it sooner than you expect." - Gartner[e]

Research shows **86%** of businesses currently reaping the benefits of better customer experience through AI. - Forbes[f].

64% of survey respondents reported they find technology landscape for AIOps solutions "confusing". - DEJ[g]

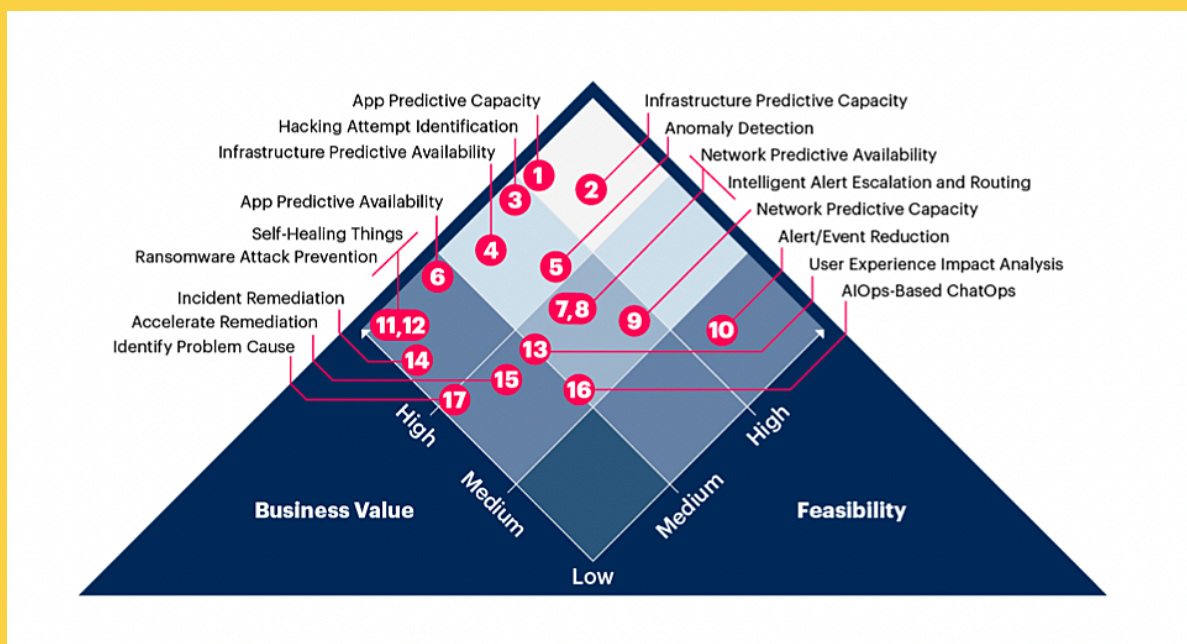
84% of survey respondents see AIOps as a path to a fully automated network environment. - Comcast business[j]

According to the recent ManageEngine ITOM survey,

3 in 10 IT admins reckon that transition from traditional to modern technology is difficult.

25% are worried about moving towards data-driven IT operations.

Gartner's AI use case prism for AIOps[h] lists 17 use cases that I&O leaders can leverage to identify the best AIOps use cases for their organizations based on each use case's feasibility and business value.













The build vs. buy conundrum: 10 factors to consider

With the implementation of AIOps becoming more of a necessity than a luxury, the next debate is, **"should we build or buy our AIOps solution?"**

As suggested by several early adopters of AIOps, the sooner the implementation quicker the ROI. At this rapid phase of technological evolution, what is modern and robust now might become clunky and outdated in a couple of years. This makes it explicit that whether an organization should build an in-house DIY AIOps solution or buy it, ultimately depends on how much time the organization is willing to spend on its AIOps solution development and implementation before it could reap its benefits.

Not just time, but here are 10 critical factors organizations should consider before deciding to build or buy their AIOps solution.

10 factors to consider before making your build or buy decision		
Factor	Build	Buy
 Cost	<ul style="list-style-type: none">Requires massive CapEx investments and high OpEx budget allocations.	<ul style="list-style-type: none">Transparent licensing and maintenance cost of solutions with built-in AIOps capabilities curb implementation costs.
 Team	<ul style="list-style-type: none">Need for expertise: Highly skilled AI, ML, and big data implementation experts with a good understanding of the mathematical models deployed. Advanced analytics talent helps reduce the AIOps' AI and ML models' error margins.	<ul style="list-style-type: none">Solution support: The learning curve of effectively reaping the benefits of built-in AIOps varies from vendor to vendor. IT teams require sufficient vendor support to successfully deploy and run the AIOps solution in their environment.
	<ul style="list-style-type: none">Training: Major stakeholders and IT operators need to be trained on understanding and utilizing the insights delivered by the AIOps platform.Culture fit: Deploying AIOps requires high collaboration enablement across teams to lay out the fundamentals such as setting-up data collection mechanisms and deciding on desired strategic outcomes. Open communication, clear goals and vision, cross-functional collaboration, and willingness to pivot from traditional practices, are some of the cultural requirements for organizations looking to start their AIOps journey.	
 Data	<ul style="list-style-type: none">Data governance: Carefully constructed data collection mechanism from well structured data lakes, meshes, and warehouses is required for full coverage data ingestion to the AIOps engine.Data collection requirements: Enhanced observability, open telemetry implementations, and full-stack monitoring.	<ul style="list-style-type: none">Leaveraging the solution's data collection capabilities: Observability and monitoring solutions collect required data on their own.
	<ul style="list-style-type: none">Data storage and retention: Provisions for ingested data storage and retention for historical analysis, pattern recognition, fine-tuning, and improvement are additionally required.	
 Hardware requirements	<ul style="list-style-type: none">DIY AIOps models run heavy workloads on the underlying hardware. To effectively sustain these high workloads and ensure process continuity, organizations should implement,	<ul style="list-style-type: none">Deploying a solution with built in AIOps capabilities requires IT teams to ensure that the specified hardware and software requirements are sufficiently met. Baseline hardware requirements can differ from vendor to vendor.

	<ul style="list-style-type: none"> • State-of-the-art high performance CPUs and GPUs. • Resilient SSD storage and memory. • Power supply system that can meet the combined thermal design point (TDP) of all deployed hardware components. 	
 Integrations	<ul style="list-style-type: none"> • The AIOps models developed should have required integrations with other alerting, orchestration, and ticketing solutions to effectively communicate the results, metrics, and insights from the AIOps engine and automate required processes. This requires deploying integration adopters across your IT infrastructure. 	<ul style="list-style-type: none"> • Usually, siloed and integrated solutions offer varied integration options for effectively communicating monitored metrics, alerts, and incident recommendations. Organizations need to ensure that they carefully choose and implement these integrations based on their desired business output and budget constraints.
 Security	<ul style="list-style-type: none"> • System integrity, vulnerability prevention, and compliance adherence are causes of concerns when it comes to DIY solutions. 	<ul style="list-style-type: none"> • SLAs and other compliance policies established between the vendor and organization enables efficiently enhanced security.
 Establishing strategic outcomes	<ul style="list-style-type: none"> • Decode the need for AIOps and clearly develop the problem statement. • Establish required business and networking outcomes of building and deploying an AIOps solution. • List the required AIOps features and capabilities to achieve the desired outcomes. 	
	<ul style="list-style-type: none"> • Communicate the established strategic outcome requirements with the in-house AIOps team to custom build the AIOps solution. • Iteratively test and improve the strategic outcomes delivery of the AIOps solution. 	<ul style="list-style-type: none"> • Examine the current and planned future capabilities offered by solution vendors and choose the solution that closely aligns with required strategic outcomes. • Leverage vendor support to scale and customize existing capabilities to custom fit your needs.
 Deployment complexity	<ul style="list-style-type: none"> • DIY AIOps solutions are comparatively highly complex to deploy and maintain. 	<ul style="list-style-type: none"> • Vendor solutions pose comparatively low deployment complexity.
 Version upgrade	<ul style="list-style-type: none"> • Migrating to a better or higher version might lead to configuration error, loss of backward compatibility, AIOps instability, and other issues without the right mechanism in place. 	<ul style="list-style-type: none"> • Migrating to higher versions of vendor solutions is seamless and easier with the vendor support, service packs, and documentation.
 AIOps capability enhancement and maintenance	<ul style="list-style-type: none"> • To keep up with the changing trends and market requirements, AIOps platform need to continually evolve to stay relevant. This levies high innovation and R&D costs from the AIOps developers. 	
	<ul style="list-style-type: none"> • Heavy R&D investments for AIOps can strain organization's IT budget. • Continued training and upskilling of the AIOps team to develop desired capabilities. 	<ul style="list-style-type: none"> • Choose vendors who offer constant solution updates, patches, and fixes to stay relevant with the changing IT landscape.

DIY AIOps foundational requirements and abstract architecture

Data is the basis for any AIOps solution to function. Along with the network's sensory data, the AIOps solution should also be fed with the network's metadata that provides the context to the processed and analyzed sensory data. The data ingested into the AIOps engine through the collectors is then processed and used to trigger advanced automation that helps organizations achieve their key technological and business objectives.

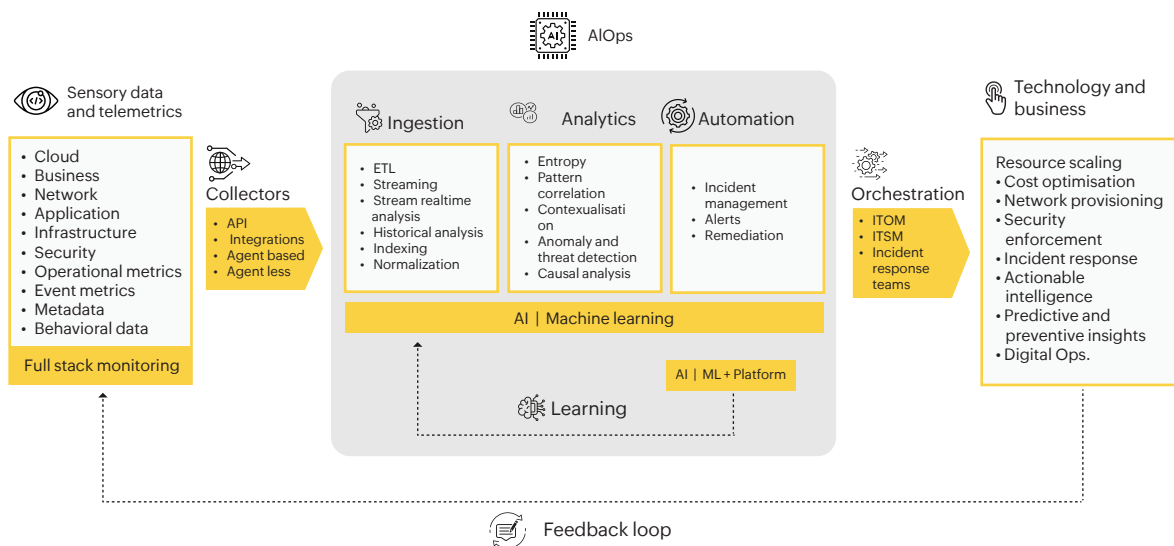


Fig 4.a, AIOps abstract architecture

Organization's looking to build their own AIOps platform should,

- **Step 1: Enable observability by setting up full stack monitoring and data collection**

This requires organizations to deploy well-structured data governance strategies that simplify data ingestion to the AIOps engine. Full stack monitoring and observability should enable visibility into the entire IT infrastructure, its sensory data, metrics, logs, and traces.

- **Step 2: Manage data collection, ingestion, and storage**

Investments in network observability and full-stack monitoring payoff during the data collection stage. Network admins need to implement instrumentation to enable open telemetry (joint vendor agnostic telemetry specification of the open census and open tracing open-sourced projects). Fully leverage the capabilities of the data transport layer to stream data from various parts of the IT infrastructure including hardware, network, cloud microservices, hybrid, and virtual environments, to the AIOps engine. Ensure sufficient storage facilities to store historical data.

- **Step 3: Setting up the AIOps engine**

This is the core and challenging part of building your own AIOps solution. Alongside conventional trend analysis and anomaly detection, organizations should also be able to build specific mathematical models enhanced by AI and

ML to deliver desired KPI and business outcomes. AI and ML subject expertise is required to set up effective and efficient analytics and hyper-automation models. To make sense of the AIOps outcomes, the user platforms or UI should be designed to display the analyzed results, outcomes, and alerts.

▪ **Step 4: External integrations with orchestration and ticketing solutions**

To reap the benefits of the AIOps engine, organizations should be able to integrate their solution with other network orchestration and ticketing tools. This includes run books, workflow tools, scripts, ITSM tools, and alerting software.

▪ **Step 5: Realizing use cases and refining business KPIs**

Building AIOps is not a one-time process. Organizations should continually improve their solution capabilities by enabling neural learning feedback, external operations based on supervised learning, and fine-tuning based on required business outcomes.

AIOps implementation maturity and business process impact

An important part of a robust AIOps strategy is regularly assessing its development and the IT infrastructure's progress toward achieving the determined key business and networking outcomes. The following AIOps maturity model aids in the periodic AIOps implementation assessment which helps organizations fine-tune their AIOps journey and growth plans to better suit their envisioned requirements.

Implementing AIOps depends on the organization's technical capabilities and desired business value outcomes. The given maturity model focuses on the organization's approach toward implementing and scaling AIOps and the reciprocated benefits in the form of process optimizations.

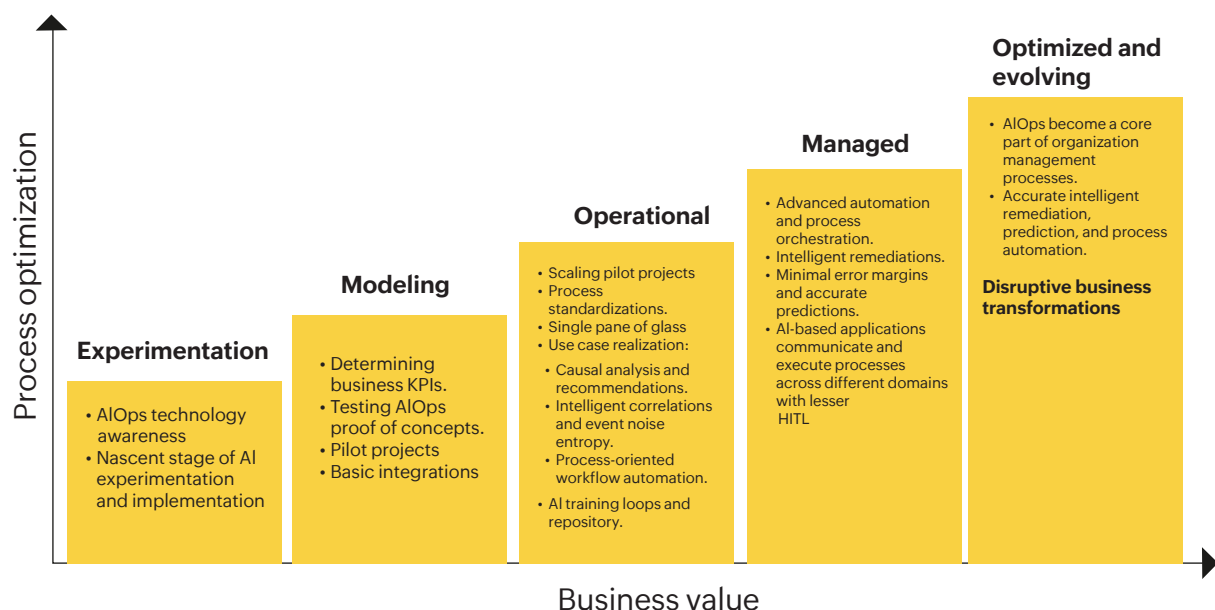


Fig 4.b, AIOps maturity model

AIOps maturity stages:

- **Experimentation:** At this stage, while organizations are aware and have recognized the need for AIOps, they are still dependent on the reactive processes to resolve network issues as enabled by their siloed monitoring solution. Only selective network data is analyzed with poor to no pattern recognition and event correlation techniques.
 - **Problem recognition** is a strong aspect of this stage where organizations question if a certain problems can be solved with AI-based implementations.
 - Organization teams start with nascent experimentation with implementing AI capabilities for particular processes. Most implementations are **ad hoc** and there is little or no AIOps benefits reaped at this stage.
- **Modeling:** This stage is characterized by having a higher level of AIOps implementation but in isolated business silos. Organizations stepping into this stage begin with evaluating the impact and outcome of their experiments. Based on their learning, the cross-functional teams involved in implementing AIOps determine business KPIs for their domain and test select process intelligence.
 - **Pilot projects:** Post-testing AIOps proof of concepts, organizations implement pilot projects and AIOps is implemented in silos.
 - There is basic integration and limited data sharing between AIOps implementation.
- **Operational:** At this stage, pilot projects are successfully scaled organization-wide along with process standardization. The AIOps implementation is "well defined" and a single pane of glass view is enabled for teams willing to leverage the results of the AIOps implementation.
 - **Use case realization:** With the organization-wide standard implementation of AIOps processes, businesses start to realize the desired holistic business outcomes.
 - **AI training loops:** Organizations fully implement AI training loops and scale their knowledge repository to make the AIOps platform more efficient and effective.
- **Managed:** Organizations are highly proactive with advanced process automation and orchestrations. AIOps is consistently and fully implemented across the organization and has become an integral part of its monitoring tasks. The AIOps platform has lesser error margins and is continually improved with a reduced need for HITL.
- **Optimized and evolving:** At this stage, organizations have adopted AIOps as a core part of their business and consider it as a value driver. Being accurate, and intelligent, AIOps offer organizations advanced and sophisticated process optimizations and automation. Organizations are ready for the next big disruptive business transformation enabled by fully implementing AIOps.

Please note: The maturity model discussed is based on the assessment by ManageEngine ITOM's analysts. How organizations choose to position themselves at different stages can differ from infrastructures, the desired business outcomes expected of AIOps, and their sole discretion.

AIOps implementation challenges

Given the advantageous functionalities of AIOps, the technology is still in its first generation and is not mature enough to be a hassle-free plug-and-play solution. Deploying an AIOps solution that can be seamlessly incorporated into existing IT infrastructures is still a challenge.

According to a recent survey,

*Over **50%** of the respondents agreed that AIOps was “challenging” or “very difficult” to implement.[i]*

Here are five challenges that make implementing AIOps in today's modern IT infrastructures, challenging.

1. Data Ops

Data determines the effectiveness, capability, and end results earned by deploying an AIOps solution. However, this first step to implementing AIOps can be a challenge for organizations that do not have well-structured data collection mechanisms in place. This includes appropriate data collection configuration, open telemetry, APIs, and integrations that enable a steady inflow of data. Good quality, full coverage, and a constant inflow of data ensure AIOps effectiveness. Unavailability and poor data quality affect the AIOps' temporal analysis capability and can lead to inaccurate results.

According to a recent survey,

Data issues are the second biggest hurdle to successful AIOps deployments, after cost.[i]

Since there is no one tool to collect all data, organizations have to rely on siloed approaches to collect and correlate data from disparate sources. This shoots up the storage and data management costs significantly. There is an indispensable need for efficient data collection and management processes that ensure full-stack network visibility and avoid network blind spots.

2. Dependency on legacy applications and systems

Lack of integration capabilities, limited scope for modernization and scaling, and outdated data logging and storage approaches have made legacy systems significant impedes to AIOps implementation.

Data collection in legacy systems often requires custom codes and integrations with third-party APIs, with no guarantee of accurate data extraction and ingestion. Also, the limited scope of automation supported by legacy systems obstructs the process efficiencies leveraged from implementing AIOps.

According to a recent survey,

35% of organizations are weary of integrating automations with legacy systems.

3. Initial learning in DIY AIOps systems

With artificial intelligence, learning matures with time and historical data stored. This is a challenging factor that requires careful attention from the CIOs before choosing to build their own AIOps platform.

During its initial stages, where the learnings of the DIY AIOps systems are from manual use case-based training and primitive data analysis, AIOps systems are prone to higher margins of error. To avoid such a scenario, organizations need to deploy intense ML model training with the aid of templates, synthetic testing, and the aid of third-party vendors and AI and ML solution providers.

4. Need for business specific strategy

With AIOps, one size does not fit all. Organizations need a clear business-specific strategy to implement AIOps and gain desired benefits. More than a "modernization" implementation, AIOps should be a "value-based implementation" in organizations.

While it is true that there is no future for ITOM without AIOps in it, while implementing AIOps, organizations should also monitor their costs to prevent them from skyrocketing.

The AIOps implementation strategy should be modeled on required productivity outcomes. For example, while AIOps promises enhanced anomaly detection, organizations can still enable entity-centric anomaly detection better with conventional monitoring tools.

5. AIOps is still learning and still improving

AIOps brings immense promise to improve the efficiencies of ITOps. As discussed, organizations that are early adopters have benefited from significant process improvements and efficiencies. However, there are some downsides to having your ITOM processes rely entirely on AIOps. At least for now.

With every AIOps vendor building and offering their version of the technology, some cloud-heavy and some on-premises-heavy, there is still some standardization required to make AIOps easy to adopt and migrate from.

For instance, vendor migration can be tediously difficult. Some early adopters became dependent on a specific vendor, and the more developed their AIOps models, the more difficult it was to migrate away from that vendor. This is the situation known as "vendor lock-in". Algorithm outcomes mature with learning, with no learning transfer standardization and reliable practices in place, migrating to a different vendor might require organizations to start from square one again. Also, while enhanced pattern recognition, data correlation, and incident management make AIOps promising for ITOM, zero-day events can still go undetected.

Chapter 5: The AIOps market and what to expect

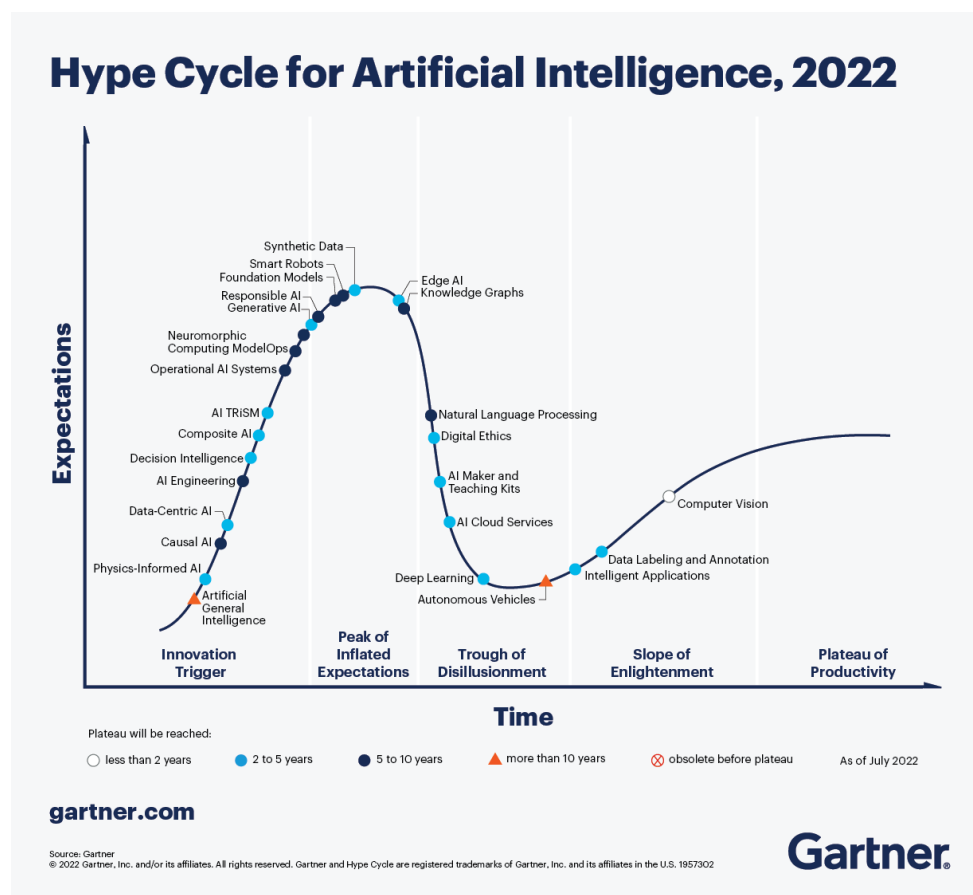
AIOps: The past, present, and future

AI and ML have been applied alongside big data analytics to simplify ITOM long before Gartner even coined the term AIOps in 2016. These were applied isolated or in parts across specific networking units such as data centers. Organizations were largely dependent on siloed monitoring resources that increased tool sprawl and simply served as beacons to indicate that an issue was detected.

The introduction of AIOps and the SaaS industry's continued collective efforts to standardize, simplify, and commoditize AIOps solutions have boosted the hype around AIOps.

AIOps market: The hype cycle and market growth over the years

"You cannot fix what you can't see" was the punch line that opened up organizations to achieve observability and implement open telemetry. But, with that came the data tsunami that flooded IT admins. A solution that was pitched as a savior? AIOps. Promising enviable capabilities including big data analytics, cutting through the noise, hyper-automation, effective incident management, and proactive remediation, the introduction of AIOps was met with accelerated adoption.



AIOps solution's market growth

Currently, at its peak of inflated expectations, AIOps solutions are being adopted worldwide despite the pandemic aftermath and the slow economy.

According to a recent market analysis[m], The AIOps platform market size is expected to grow from \$2.83 Billion in 2021 to \$19.93 Billion by 2028; it is estimated to grow at a CAGR of 32.2% from 2021 to 2028.

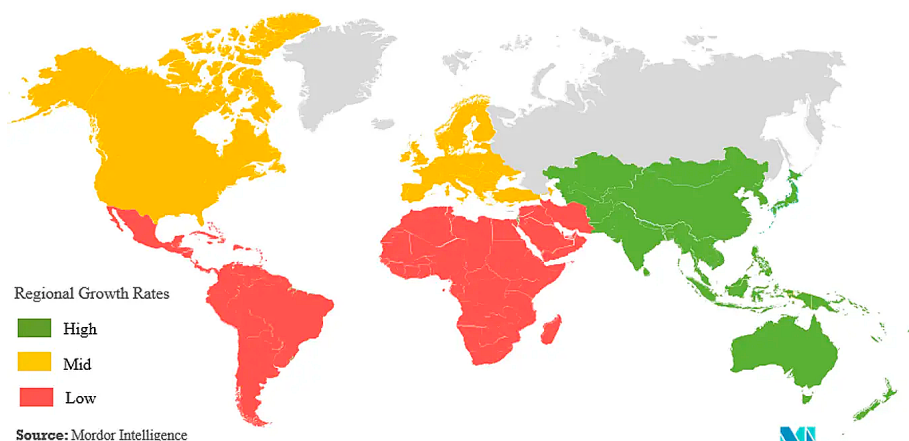
Major market segments: AIOps has been adopted widely across all sectors including information technology, telecom, banking, financial services and insurance, healthcare, retail, media and entertainment, government, and manufacturing.

ITOM market: The most widely reported AI adoption (47%) was in the IT and technology sector, followed by R&D with 36%, and customer service with 24%. This signifies the growing importance given to AI in the IT operations field[l].

Market growth by region: The AIOps market is continuing to experience high adoption rates in the APAC region, followed by Europe and North America. Latin America followed by Africa experiencing slower adoptions rates.

- **North America and the booming R&D:** Being a thriving SaaS hub, this region's adoption of AIOps is fueled by substantial R&D investments and market development by AIOps vendors. Organization's accelerated digital transformation initiatives have also boosted the need for AIOps adoption.
- **Europe region—MSPs:** One of the primary reasons for the growth of the AIOps market in Europe is the region's MSPs seeking to offer comprehensive services to enterprises undergoing large-scale digital transformation and requiring modern operations solutions.
- **APAC region:** Projected to be one of the most significant markets for AIOps, the region's AIOps adoption is accelerated by several factors including COVID-19 pandemic and remote work, a booming start-up culture, and the need to optimize infrastructure operations.

AIOps Market - Growth Rate by Region (2021 - 2026)



A look into AIOps' future: What to expect?

Implementing advanced consciousness, self-healing systems, and complete autonomous functioning are goals that likely won't be achieved for some time. AIOps solutions providers and their R&D teams are currently on the road to achieving reduced error margins, enhanced efficiency, accurate predictions, and actionable remediation. But that doesn't make the future AIOps anywhere close to being bleak. The impending trough of disillusionment, while not an entirely sweet reality, holds the immense promise of efficiency and process improvement.

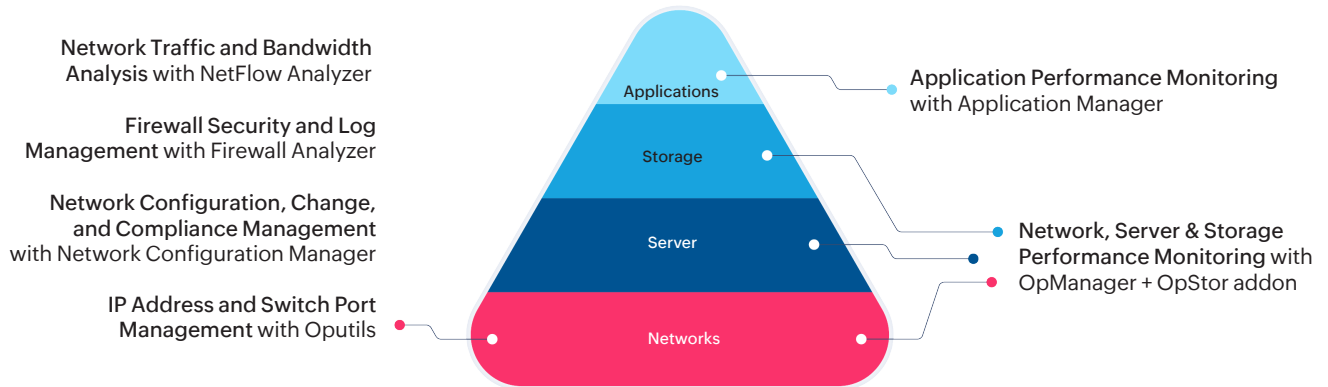
Some of the AIOps capabilities to look forwards to in the future,

- **Advanced automation and better data ops:** Organizations can expect data collection to become an integral part of the AIOps platform. Enhanced data management automation capabilities, such as intelligent data automation fabrics, promise an efficient alternative for arduous data ops which is currently a challenge to implementing AIOps.
- **Enhanced deep learning:** This involves heavy R&D investments from vendors and organizations to improve the accuracy, diversity, and effectiveness of the ML models. This results in an increased probability that advanced deep learning will be integrated into AIOps. More mature ML models can further increase the ROI and business outcomes delivered by the AIOps platforms.
- **Refined automated decision-making:** Currently, most AIOps platforms operate on observing external operant inputs and HITL. Advances in the field of deep learning and neural networks can move AIOps solutions from being human intelligence augmenters to automated decision makers. This enhanced ability to function autonomously can aid in tackling the issues currently faced, such as prompt detection of zero-day events, and detecting data quality issues.
- **Standardizing solution migration and integration:** As discussed in the implementation challenges, currently, AIOps solutions are difficult to migrate from causing vendor lock-in and knowledge loss. As the industry matures and vendors evolve, organizations can expect better migration, knowledge transfer, and integration capabilities.
- **Security enhancements:** Organizations can expect enhanced security functionalities including the ability to detect network attacks, Trojans, and intrusions. Enhanced security capabilities can significantly reduce the organization's risk vectors and enable security-centric remediation to proactively secure IT infrastructures.

About ManageEngine ITOM

With over 16 years of expertise in simplifying ITOps for complex infrastructures, ManageEngine ITOM solutions are trusted by over 1 million IT professionals across 185 countries. Recognized by leading research and market analyst firms including Gartner, EMA, and InfoTech, ManageEngine ITOM solutions are the proud recipient of several notable customer awards and reviews. With a unified approach to ITOps, our solutions have enabled businesses to achieve complete visibility, full-stack monitoring, and uninterrupted network availability across distributed architectures, virtual environments, and data centers.

Our solutions: Everything you need to gain full stack visibility into your network



ManageEngine OpManager: Network, server, and storage performance monitoring

Deployment: On-premises | MSP

Proactively monitor your critical network resources' availability, health, and performance metrics with more than 2,000 built-in network monitors. With its robust network monitoring capability, enable enhanced network performance, fault management, complete network visibility, constant network availability, and avoid costly network downtime.

Feature highlights:

- Network devices monitoring
- Physical and virtual server monitoring
- Multi-site and distributed network monitoring
- Hardware monitoring
- Alarms and notifications
- Workflow automation
- Failover and high availability

ManageEngine Applications Manager: Applications and server performance monitoring

Deployment: On-premises

Enhance performance and user experience of your heterogeneous set of business critical applications across physical, virtual, and cloud environments. Get code level insights, automation capabilities, and out-of-the-box support for over 150 technologies that enable you to ensure seamless user experience for your end users.

Feature highlights:

- Application Discovery and Dependency Mapping (ADDM)
- Synthetic transaction monitoring
- End-user experience monitoring
- Fault management with root cause analysis
- Anomaly detection with dynamic base lining
- Advanced analytics to generate reports

ManageEngine NetFlow Analyzer: Network traffic and bandwidth analysis

Deployment: On-premises

Get in-depth insights into the network traffic and bandwidth consumption with support for leading flow technologies. Perform network forensics, analyze network flows, track traffic network forensics, analyze network flows, track traffic consumption, and optimize bandwidth utilization alongside securing your network with advanced security analytics.

Feature highlights:

- Network bandwidth monitoring
- Network traffic monitoring
- Faster network troubleshooting
- Threshold based alerting
- Integrated network management

ManageEngine Network Configuration Manager: Configuration, change, and compliance management

Deployment: On-premises

A network configuration and change management solution that offers you complete control over your network configurations and compliance. Gain insights into who, what, and when of configurations and changes, conduct remote network operations with Configlets, leverage automated configuration backups, and enable customizable compliance policies to avoid violations.

Feature highlights:

- Automated backups
- Change management in real time
- Compliance monitoring
- Configlets
- Task automation
- Extensive reports

ManageEngine Firewall Analyzer: Firewall security and log management

Deployment: On-premises

With support to over 50 firewall vendors, Firewall Analyzer is a firewall log analytics and configuration management software that enables you to enhance network security by offering in depth insights in to the firewall policy, user internet activity, log analysis, and network forensic audits.

Feature highlights:

- Firewall Policy Optimization Report
- VPN Reports
- Employee Internet Usage
- Firewall Used Rules Report
- Firewall Alerts
- Virus, Attack, and Security Reports

ManageEngine OpUtils: IP address and switch port management

Deployment: On-premises

OpUtils is a comprehensive IP address management software that enables you to track your network address space availability and utilization across multiple subnets, supernets, and DHCP server scopes. With support for IPv4 and IPv6 addressing, OpUtils also enables switch port mapping that offers details in to the MAC devices network connectivity and helps enhance network security with its rogue detection capabilities.

Feature highlights:

- IP Address Management
- DHCP scope monitoring
- Switch Port Management
- Rogue Device Detection
- More than 30 network tools

ManageEngine OpManager Plus: Unified IT operations management

Deployment: On-premises

This all-in-one IT operations management software offers an unified approach to monitoring your network performance, application experience, bandwidth consumption, configurations, changes, and compliance, along with firewall, IP address, and switch port management.

Feature highlights:

- Server monitoring
- Bandwidth management
- Network configuration management
- Firewall log management
- IP address and switch port management
- Application management

Take your first step towards adaptive, fast-paced, AI-enabled ITOps with ManageEngine ITOM solutions today.

Glossary

Term	Definition
ADDM	Application discovery and dependency mapping
AI	Artificial intelligence
AIOps	Artificial intelligence for IT operations
APAC	Asia-Pacific region
API	Application programming interface
CAGR	Compound annual growth rate
CapEx	Capital expenditure
CIOs	Chief information officers
DDM	Discovery and dependency mapping
DevOps	A term combining application "development" and IT "operations"
DHCP	Dynamic host configuration protocol
DIY	Do-it-yourself
GPU	Graphics processing unit
HITL	Human in the loop
I&O	Infrastructure and operations
IaC	Infrastrucutre as code
KPI	Key performance indicators
ITOM	IT operations management
ITOps	IT operations
ITSM	IT service management
ML	Machine learning
MSP	Managed service provider
MTBF	Mean time between failures
MTTD	Mean time to detect
MTTF	Mean time to failure
MTTK	Mean time to know
MTTR	Mean time to repair
OpEx	Operational expenditure
R&D	Research and development
RBA	Rule-based automation
RCA	Root cause analysis
ROI	Return on investment
SLA	Service-level agreement
SRE	Site reliability engineer
SSD	Solid-state drive
TDP	Thermal design point
VPN	Virtual private network

Reference:

In text:

- [a] <https://www.gartner.com/en/documents/4000217>
- [b] <https://www.fastly.com/web-application-and-api-security-tipping-point>
- [c] <https://itic-corp.com/tag/hourly-cost-of-downtime/>
- [d] <https://www.dej.cognanta.com/2020/05/04/the-aiops-maturity-research-study-key-findings/>
- [e] <https://www.gartner.com/smarterwithgartner/how-to-get-started-with-aiops>
- [f] <https://www.forbes.com/sites/tomtaulli/2020/12/12/artificial-intelligence-ai-whats-in-store-for-2021/?sh=5ac9a6c55a3c>
- [g] <https://www.dej.cognanta.com/2020/05/04/the-aiops-maturity-research-study-key-findings/>
- [h] <https://www.gartner.com/en/documents/3994888>
- [i] [https://www.enterprisemanagement.com/research/asset.php/4056/AI\(work\)Ops-2021:-The-State-of-AIOps](https://www.enterprisemanagement.com/research/asset.php/4056/AI(work)Ops-2021:-The-State-of-AIOps)
- [j] <https://www.masergy.com/white-paper/2021-state-of-aiops-study>
- [k] <https://www.gartner.com/en/articles/what-s-new-in-artificial-intelligence-from-the-2022-gartner-hype-cycle>
- [l] <https://www.mordorintelligence.com/industry-reports/aiops-market>
- [m] <https://www.theinsightpartners.com/reports/aiops-platform-market/>

Image:

- [1] <https://fortune.com/2021/10/04/facebook-outage-cost-revenue-instagram-whatsapp-not-working-stock/>
- [2] <https://www.wsj.com/articles/amazon-finds-the-cause-of-its-aws-outage-a-typo-1488490506>
- [3] <https://www.alphr.com/software/1000494/app-store-outage-cost-apple-over-17-million/>
- [4] <https://www.businesswire.com/news/home/20220928005357/en/Half-of-Large-Enterprises-Hit-by-Financial-Losses-Due-to-Net-work-Outages>
- [5] <https://uptimeinstitute.com/about-ui/press-releases/2022-outage-analysis-finds-downtime-costs-and-consequences-worsening>

About the author



Sharon A Ratna
Product consultant

Sharon A Ratna is a Product consultant for ManageEngine's ITOM suite that has helped IT teams in Fortune 100 worldwide for over 20 years. She researches and writes on technologies that develop, enhance, and simplify the current solution capabilities and new opportunities in the ITOM domain. With an exceptional understanding of marketing trends and consumer pain points, she works with the product management, development, and support teams to fine-tune and execute engaging marketing strategies. A passionate storyteller, in her free time enjoys reading books and traveling.