Moogsoft®

AIOPS BUYER'S GUIDE

THIS BUYER'S GUIDE will help you better understand the benefits you can expect from investing in an AIOps platform.

Before evaluating vendors, it's important that you first understand your organization's core challenges, identify the sources of those challenges, isolate the key functional areas you need to address, and establish the product capabilities that are required to meet your business needs.

Following this process, and consulting the information found in this guide, will help you identify which AIOps vendors you should select to evaluate, and, more importantly, will help ensure that you get the answers needed to help you reach your goals and get the most out of your AIOps investment.

Defining AIOps

AIOps is a category defined by Gartner Research, and stands for "Artificial Intelligence for IT Operations." You can think of this category as an evolution of IT Operations Analytics (ITOA), through which AIOps is the application of algorithms that utilize AI and machine-learning techniques to deliver insights (e.g. analytics). These insights are required by teams as diverse as ITOps, DevOps, Site Reliability Engineering, and Application Support. The primary purpose of AIOps platforms is to help these teams automate time-consuming and error-prone tasks, in turn making human operators faster, smarter, and more proactive in how they manage the performance and availability of digital services.

The algorithms behind AIOps benefit complex IT organizations that experience frequent change and high degrees of unpredictability by automatically understanding significance and patterns, without being explicitly told what to look for. This relieves organizations from the burden of modeling all failure scenarios and constantly updating those models over time. Furthermore, the capabilities of these algorithms tremendously exceed the capabilities of human cognition when it comes to speed, scale, and precision.

By automating the analysis of all monitoring telemetry (Events, Alerts, Syslog, SNMP TRAP, etc.), enabling correlation and visibility across toolsets, and providing service-impact analysis, organizations that invest in AIOps can expect increased agility, lower cost of operations, and improved customer experience.

While the benefits of AIOps have been proven in many of the largest and most complex IT environments in the world, the technology is still relatively early in its adoption globally. However, Gartner Research predicts that by 2022, 40% of enterprises around the world will be using AIOps platforms to support their operations . The opportunity to experience the benefits of early adoption is real, and businesses that utilize AIOps technology will have a competitive advantage over late movers.

Focus on Business Value, Not Features

Unfortunately, nearly every IT monitoring/management vendor claims to utilize AI, data science, and machine-learning capabilities within their product to improve your operations. Many buyers are rightfully skeptical of these claims, and there is a non-trivial amount of confusion in the market, which makes it difficult for buyers to separate fact from marketing fiction.

The truth is, no single vendor does everything well. Many vendors simply stick words like "machine learning" and "AI" in their marketing materials in an effort to appeal to a growing audience, yet don't really have the capabilities needed to make their customers successful. In fact, many AIOps vendors offer nothing more than the same rules and behavioral model-based approaches that were used in the 1990s.

When considering AIOps technologies, the first and most important step is to identify the key problems you want to solve, and start your conversation with vendors around business value, not features. While AIOps can be transformational to your business, it likely isn't a cure for every issue affecting your operations. So take the time to understand the implications of the technology on your business, and be careful to avoid "technology for technology's sake."

Avoid technology for technology's sake.

Identify the Key Challenges You are Trying to Solve

Aside from the overarching goals of improving the performance and availability of your services, there are likely several more concrete challenges that are leading you to consider investing in AIOps.

Before evaluating any AIOps solutions, you need to identify the major challenges you are hoping to solve through AIOps. You will need to refer back to these challenges throughout your AIOps evaluation process.

Avoid getting sidetracked by cool buzzwords, technology, and features. At the end of the day, AIOps costs money, and you will have to justify any spend with real business value.

Typical Challenges in Modern Operations Environments

1. Too much event volume, noise, and duplication
2. Lack of context and visibility across tools
3. Team silos and under-optimized collaboration
4. Reactive workflow (e.g. customers report incidents before ops identifies them)
5. Growing cost of support and operations
6. A lack of agility and an inability of operations to keep up with pace of change in the business
7. Decentralization of operations and lack of specialization or domain expertise

Identify the Source of These Challenges

The challenges you face today probably didn't appear overnight. To surface the underlying sources of your challenges, take a few minutes to perform this simple exercise: Write down your core challenges and ask "Why?" five times for each challenge.

As an example:
We have too much downtime.

Why? *Our teams struggle to detect incidents in production, and are way too reactive.*

Why? *Our operators spend hours manually analyzing/correlating alerts across our production stack.*

Why? *We have a signal to noise problem; operators are overwhelmed with event/alerts.*

Why? *We have 20+ disparate monitoring tools that constantly fire alerts without any context to the underlying issue.*

Why? *We lack basic alert correlation and a single-pane-of-glass view across our toolsets.*

This exercise will help you determine the underlying cause(s) of each core challenge, and will expose each of the high-level areas that you need to focus on during your AIOps evaluation.

Common Reasons Why IT Organizations have Challenges with IT Operations

- Event and alert volumes are spiraling out of control
- Lack of situational awareness across the production stack
- No single-pane-of-glass view or correlation across tools
- Too many duplicate and non-actionable tickets
- Too many bridge calls/ war rooms with too many people
- Teams troubleshoot in silos
- Lack of monitoring visibility

Assessing Low-Level Capabilities

Once you identify your core challenges and understand why they exist, you can then drill-down on each functional area to discover the specific capabilities that you require.

Here are some common AIOps functional areas and their underlying low-level capabilities:

NOISE REDUCTION

- Filters
- Deduplication
- Blacklisting
- Whitelisting
- Algorithmic Signal:Noise Detection

EVENT CORRELATION

- Custom Rules - to detect 'exact' matches
- Supervised Machine Learning - to detect previously experienced behavior
- Unsupervised Machine Learning - to detect previously unknown behavior
- Semi-supervised Learning - to detect related behavior via fuzzy matching
- Correlation across multiple Event Attributes
- Correlation across multiple Event Sources
- CMDB Enrichment for Service Impact Analysis
- Topology/Root-Cause Analysis
- Root-Cause Analysis via Neural & Supervised Machine Learning
- Neural Learning from Human Behavior for Correlation Refinement

COLLABORATION

- Virtual War Room
- Chatops
- Knowledge Capture & Recycle
- Predictive Insights
- Decision Support
- Leverage Existing Ecosystem to Unify Workflow
- SIAM (Dynamic Teaming)

ECOSYSTEM AUTOMATION

- Auto-Ticketing
- Notification/Escalation (e.g. Slack, xMatters)
- Embedded Tools
- Contextual Linking to Existing Toolsets
- Auto-Diagnostics Testing
- Enrichment for Efficient Workflow (Prioritization, Service Impact, User Impact, Location Impact, Change Windows, etc.)
- Runbook Automation

Defining Success Criteria

Without identifying what success looks like, you won't reach the full potential of what AIOps has to offer.

Simple Questions to Ask

1. What capabilities do I require to to solve these problems?
2. How do I know when these problems are solved?
3. How am I going to measure success?

Pick four or five key performance indicators (KPIs) or metrics that you can track over time to make sure AIOps is delivering on its promise. Here are some metrics that Moogsoft customers use to measure success and ROI.

It's crucial to track core KPIs or metrics before evaluating AIOps so that success can be objectively measured during and after the evaluation.

Key Performance Indicators

- Availability
- Reduction of Raw Events to Unique Alerts
- Correlation of Unique Alerts into Situations
- Tickets Volumes
- Actionability of alerts/ tickets
- # of incidents (Severity 1-4)
- # of people involved in incidents (Severity 1-4)
- Customer Identified vs. Monitoring Identified Incidents
- # of Repeated Incidents
- Mean-Time-To-Detect (MTTD), Mean-Time-To-Acknowledge (MTTA), Mean-Time-To-Resolve (MTTR)

Identifying Use Cases and Primary Users

Challenges and success must tie to real life use cases and teams within your organization. Contrary to popular belief, AIOps is about augmenting and assisting humans, not replacing them.

Who are those people? How do you expect AIOps to change their day-to-day activities? Is the scope of AIOps limited to certain use cases and teams, or are you expecting it to deliver benefits enterprise-wide?

Example Use Cases & Users:

- Incident Management – Helpdesk, L1 & Supporting Teams
- Event Management – Helpdesk & L1
- Service Management – Service Delivery & Support
- Monitoring – Enterprise Monitoring, App Support, NOC, SRE
- Detection – NOC/Helpdesk/L1, SRE
- Troubleshooting – App Support L2, SRE
- Development & Testing – App Dev, SRE
- CI/CD – DevOps, SRE
- Notification/Escalation – L1/L2
- Reporting – Exec, Biz, Architects
- Security – Security Engineers

Understanding Your Environment and Toolsets

You are now at a point where you should be asking yourself questions to determine which of the many AIOps platforms are worth evaluating. Selecting the right AIOps platforms depends on many factors, but it's crucial that you understand your own IT environment, and which AIOps platforms can support such an environment.

Every production environment is unique, and therefore, it's impossible for every AIOps platform to be a good fit for your environment. You need to identify which AIOps platforms are properly built to accommodate *your* environment.

These questions are important because any AIOps solution you evaluate is going to have to integrate and work well with the tools you already own. It's also an excellent opportunity to rationalize and validate which gaps in your current monitoring ecosystem AIOps may be able to fill.

The more traditional AIOps vendors (e.g. IBM, CA, BMC) tend to have platform/ecosystem support for their own set of toolsets, as opposed to more modern vendors, which provide support across different vendor toolsets.

Here are some of the questions you should be asking:

How many applications/services do you have?
1 | 10s | 100s | 1,000s | 10,000s

How many hosts/devices/machines do you have?
100s | 1,000s | 10,000s | 100,000s | 1,000,000+

How often does your environment change?
Seconds | Minutes | Hours | Days | Weeks

How many events/alerts are you generating a day?
Hundreds | Thousands | Millions | Billions

How many operators do you have?
<10 | 10s | 100s | 1000s

How many teams do you have?
<10 | 10s | 100s?

What tools do you currently use?

- Deployments/Releases (e.g. Chef, Puppet, Automic, ElectricCloud, Ansible)
- Application/Services (e.g. AppDynamics, New Relic, Dynatrace)
- Network (e.g. Netscout, Riverbed, Solarwinds)
- On-Premises Infra (e.g. Nagios, Zenoss, ScienceLogic)
- Cloud Infra (e.g. AWS CloudWatch, Azure X, Datadog, Wavefront)
- Log Files (e.g. Splunk, Sumologic, AppDynamics, Loggly)
- Events/Alerts (e.g. IBM Netcool, CA Spectrum, BMC TrueSight, Email)
- Tickets (e.g. BMC Remedy, ServiceNow, Cherwell, Jira)
- Notifications/Escalation (e.g. PagerDuty, XMatters, OpsGenie, VictorOps)

Deployment Options

Things to Consider

- Do you want your enterprise deployment to be multi-tenancy or dedicated?
- Are most of your current IT Operations tools deployed on-premises or via SaaS?
- Do you have any security restrictions for IT data to leave the corporate data center?
- Do you have any corporate firewalls or proxy servers that prevent HTTPS data communications to SaaS platforms?
- User authentication and RBAC – does the solution support LDAP/AD/SAML?
- What are the top three largest deployments the solution vendor supports via their on-prem/SaaS? *This is important!*

Not all vendors offer AIOps as both on-premises and SaaS software. While both options undeniably have their respective pros and cons, it should be your organizational requirements that drive this deployment decision.

This consideration alone will allow you to be much more selective in which AIOps platforms you evaluate.

Cost of Ownership vs. ROI

Cost, time-to-value, and ROI are always relative. Ask AIOps vendors to set expectations and justify those expectations based on the characteristics of your environment.

Beyond the vendors' business value analyses, you should conduct reference calls with customers in similar verticals and of similar scale to ask certain questions.

Questions to Ask

- What was the deployment level of effort?
- What was the time-to-value?
- What is the TCO? How many dedicated resources does the AIOps platform require in production?
- How flexible is the platform to change in your environment?
- What is the ROI in terms of agility, operational efficiency, service quality, customer retention, etc.?

> Cost, time-to-value, and ROI are always relative.

Evaluation Process: Key Requirements & Proof-Points

Once you understand the AIOps platforms that you wish to evaluate, the core functional areas that you want AIOps to improve, and the low-level capabilities you require to get there, you need to decide how you want to evaluate AIOps platforms to choose the best fit.

The Key Requirements checklist on the next page can be used as a guide for all key criteria within the evaluation.

Before evaluating AIOps platforms, you need to ask yourself the following questions:

- In which environment will your evaluation take place in?
- What are your data inputs going to be for AIOps? (i.e., Data Sources)
- What are your outputs going to be?
- Which teams need to be part of this evaluation?
- What is the desired timeframe for the evaluation?

In Closing

With growing interest around AIOps, along with a proliferation of solutions, purchasing the right solution for your organization is a serious challenge. We hope that this AIOps Buyers Guide simplifies your search for the right AIOps platform.

Interested in learning more?

Reach out to us for a full operational assessment to identify where AIOps can help: **info@moogsoft.com.**

Key Requirements

DEPLOYMENT OPTIONS

- ☐ SaaS
- ☐ On-Premises
- ☐ Hybrid Deployment

INTEGRATIONS

- ☐ Out-of-the-Box Integrations for key technologies
- ☐ Open Standards-based REST Web Services
- ☐ Open API to Enable and Support Custom Workflows

NOISE REDUCTION

- ☐ Filters
- ☐ De-duplication
- ☐ Blacklisting
- ☐ Whitelisting
- ☐ Algorithmic Signal-Noise Detection

CORRELATION

- ☐ Custom Rules - to detect 'exact' matches
- ☐ Supervised Machine Learning - to detect previously experienced behavior
- ☐ Unsupervised Machine Learning - to detect previously unknown behavior
- ☐ Semi-supervised Learning - to detect related behavior via fuzzy matching
- ☐ Correlation across multiple Event Attributes
- ☐ Correlation across multiple Event Sources
- ☐ CMDB Enrichment for Service Impact Analysis
- ☐ Topology/Root-Cause Analysis
- ☐ Root-Cause Analysis via Neural & Supervised Machine Learning
- ☐ Neural Learning from Human Behavior for Correlation Refinement

COLLABORATION

- ☐ Virtual War Room
- ☐ Chatops
- ☐ Knowledge Capture & Recycle
- ☐ Predictive Insights
- ☐ Decision Support
- ☐ Leverage Existing Ecosystem to Unify Workflow
- ☐ SIAM
- ☐ Dynamic Teaming

ECOSYSTEM AUTOMATION

- ☐ Auto-Ticketing
- ☐ Notification/Escalation (e.g. Slack, xMatters)
- ☐ Embedded Tools
- ☐ Contextual Linking to Existing Toolsets
- ☐ Auto-Diagnostics Testing
- ☐ Enrichment for Efficient Workflow (Prioritization, Service Impact, User Impact, Location Impact, Chage Windows, etc.)
- ☐ Runbook Automation
- ☐ Reporting

Moogsoft AIOps helps modern IT Operations and DevOps teams become smarter, faster, and more effective by providing technological supplementation that automates mundane tasks, enables scalability, and frees up human beings to do what they do best — ideate, create, and innovate.

www.moogsoft.com

1265 Battery St., San Francisco, CA 94111