

# **Get started on AIOps** without spending the big bucks

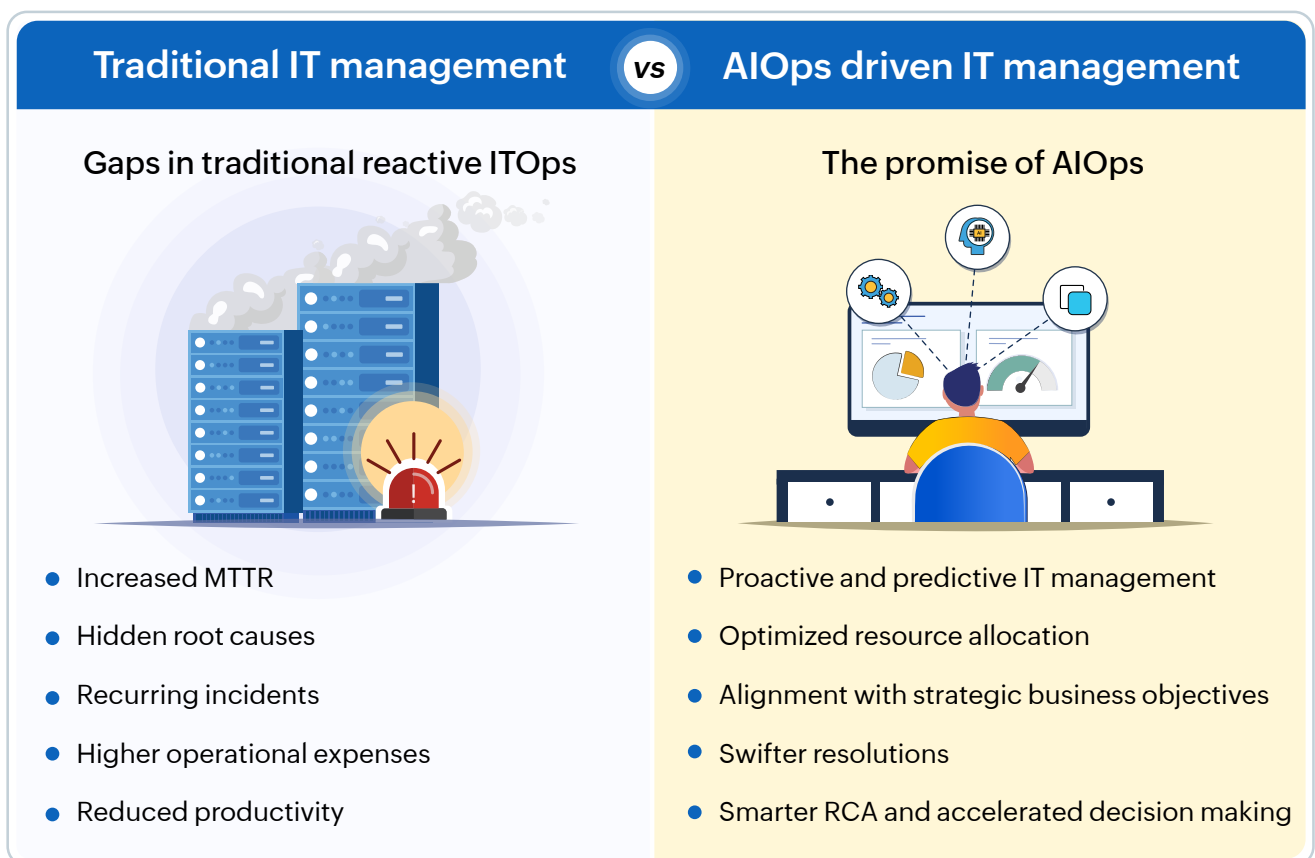
✦ A cost-effective guide to intelligent IT

# Table of contents

■	AI in IT: Ushering in an era of smarter IT operations	3
■	Proactive performance management	6
■	Intelligent incident management	9
■	Detection of insider threats from privileged accounts	12
■	Strategic capacity planning and resource cost optimization	16
■	Conclusion	19
■	About ManageEngine Analytics Plus	20

# Ushering in an era of smarter IT operations

**AI** has transcended its science fiction origins to become a transformative force within the IT landscape. This once-futuristic vision is now a tangible reality, reshaping industries globally. Its rapid growth has significantly impacted IT operations, a historically resource-intensive area fraught with inefficiencies. AI has emerged as a vital solution for managing the increasing complexity and volume of IT data, enabling organizations to keep pace with modern demands. This has fueled the rise of artificial intelligence for IT operations (AIOps). AIOps' potential is vast, and when implemented effectively, it empowers organizations to automate routine tasks, predict and prevent outages, and optimize resource allocation, thereby improving decision-making and operational efficiency.



However, many organizations find themselves at a crossroads, facing a daunting challenge: How to embrace the power of AIOps without breaking the bank?

## The quest for cost-effective AIOps

At its core, AIOps involves the strategic application of AI/ML, and data-driven analytics to monitor and enhance operations data, ultimately driving process efficiency. AIOps is evolving into an indispensable tool for automation and intelligent decision-making across various dimensions of both business and IT.

Yet, in today's efficiency-focused environment, IT leaders often worry about investing heavily in solutions that might not deliver the promised results, leading to financial strain.

For many IT teams, the AIOps journey begins with apprehension due to perceived high implementation costs and uncertain return on investment (ROI).

Furthermore, even organizations that have adopted AIOps often realize only a fraction of its potential. Many primarily use it for basic functions like:

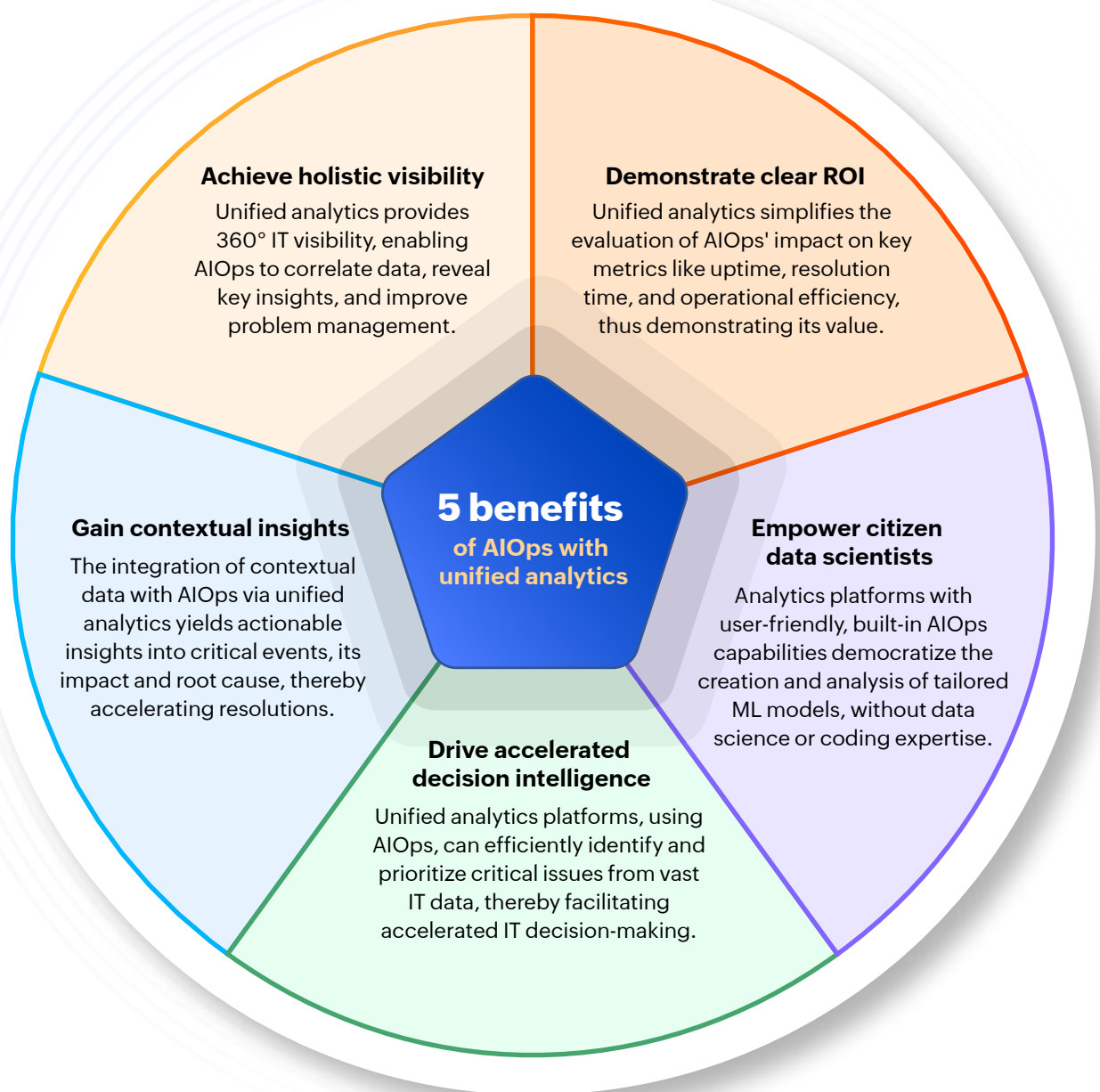
- **Alarm correlation:** Reducing alert noise by intelligently grouping related notifications.
- **Basic service availability monitoring:** Tracking the uptime of critical systems.

Additionally, organizations often use AIOps with isolated, domain-specific IT solutions. These fragmented approaches create data silos, limiting the ability to correlate insights across the entire IT environment. Consequently, they miss the opportunity to gain a holistic understanding of their interconnected systems and unlock the full power of AIOps.

## Unlocking the full potential of AIOps with unified analytics

But what if there was a way to overcome these challenges and adopt AIOps without a hefty price tag? This is where unified analytics comes into play.

Unified analytics offers a cost-effective and outcome-driven pathway to AIOps adoption. By breaking down IT data silos and providing a central platform for comprehensive analysis, unified IT analytics delivers the following benefits.



Essentially, unified analytics enables organizations to move beyond a fragmented AIOps approach to embrace a strategic, enterprise-wide solution that delivers optimal ITOps efficiency and a strong ROI. This fundamental shift fosters a more intelligent, responsive, agile, and cost-effective ITOps environment that dynamically adapts to evolving business demands.

This e-book will delve into four key IT scenarios that illustrate how the strategic and cost-effective application of AIOps within IT analytics can enable organizations to move beyond traditional monitoring and adopt a smarter, proactive approach to IT management, leading to improved efficiency, reduced IT costs and waste, and ultimately boosting the overall ROI of IT investments and efforts.

01

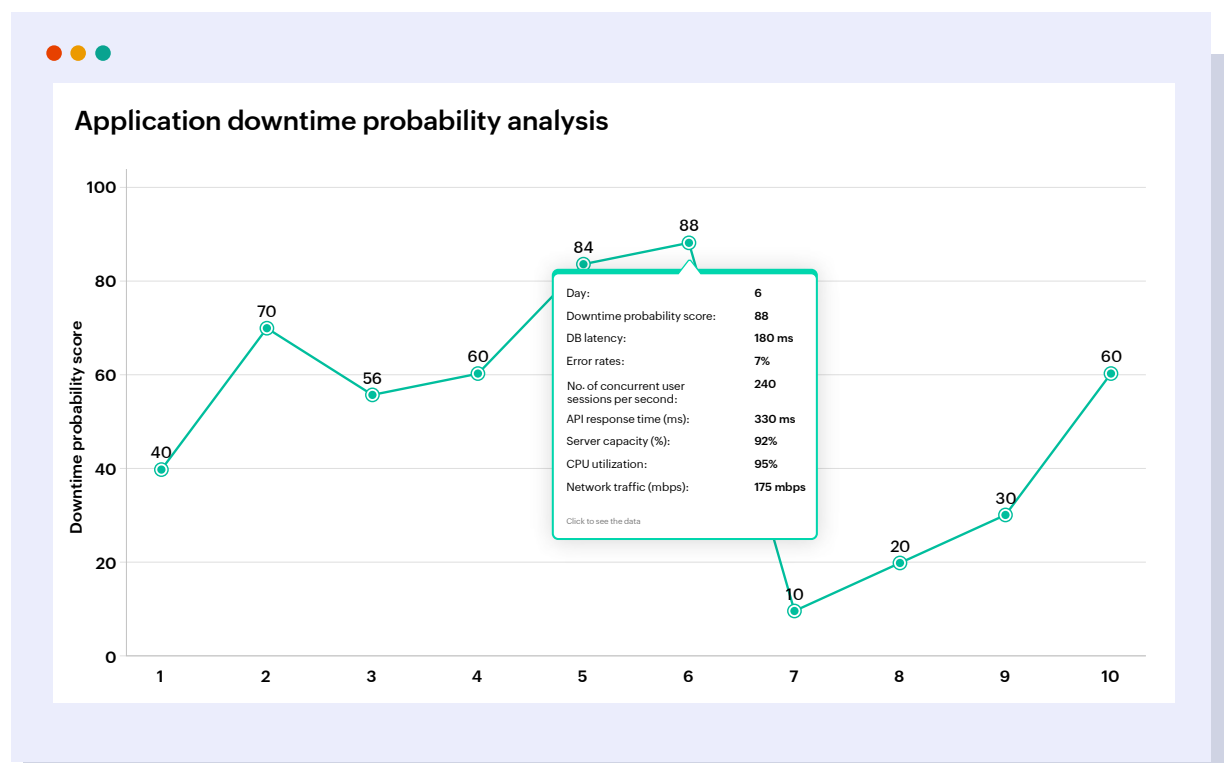
## Proactive performance management

**T**raditionally, IT teams have adopted a problem-centric approach to infrastructure and application performance—primarily reacting to performance bottlenecks only after an incident occurs. In today's fast-paced, highly competitive business environment, this reactive mindset can result in serious financial losses, operational disruptions, and reputational damage. AIOps enables a proactive shift by identifying subtle patterns and anomalies that often precede major incidents. This empowers IT teams to intervene and address performance gaps before they impact end users.

One powerful way to achieve this proactive stance is by applying tailored ML models that predict future performance issues. These custom models are trained using both real-time and historical data, enabling IT teams to forecast the likelihood of potential incidents across the IT landscape. By correlating data from diverse sources, these models provide rich, contextual insights into where and when performance issues might arise.

Analytics Plus, ManageEngine's flagship IT analytics platform, provides a no-code AutoML capability that simplifies this process. IT managers and analysts can create, train, and deploy custom ML models without needing deep coding or data science expertise. The platform enables users to select the optimal algorithm, train the model, and generate tailored insights that IT teams can act on with confidence.

Let's consider an e-commerce company preparing for a high-stakes sales event like Black Friday. In such situations, even minor application slowdowns or outages can trigger significant revenue loss, customer dissatisfaction, and reputational harm. Traditional monitoring systems might only sound the alarm when performance has already degraded. But analytics platforms with AIOps capabilities can foresee such risks well in advance.



The analysis above visualizes the trend of the application downtime probability score over 10 days during peak traffic periods.

The custom application performance model, developed using ML, leverages historical data and a range of critical operational factors like database query latency, server capacity utilization, error rates extracted from application logs, API response times, and the volume of concurrent user sessions. This accurately computes the application's downtime probability score, enabling IT teams to implement preemptive measures. IT managers can configure automated, anomaly-based alerts for days predicted to have a high downtime probability and initiate proactive remediation actions, such as:

- Auto-scaling database resources to handle anticipated traffic surges.
- Rolling back recent changes that might have introduced performance issues.
- Rerouting user traffic away from faulty network segments.
- Optimizing API performance, particularly for endpoints experiencing high response times.

By proactively identifying and addressing potential problems before they impact users, AIOps transforms performance management from a reactive firefighting exercise into a strategic, preventative practice. Through proactive performance management, IT teams can ensure uninterrupted service, especially during periods of peak demand, and reduce the number of costly outages, resulting in significant productivity as well as financial gains.

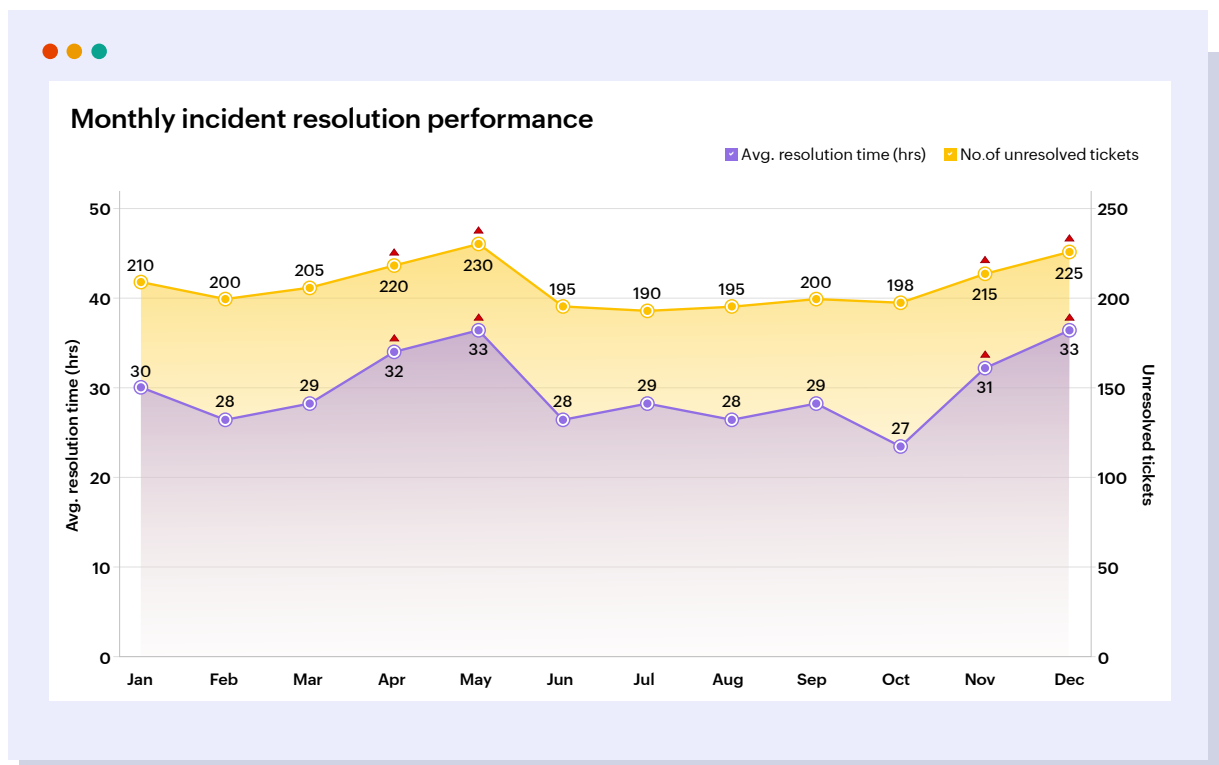


# Intelligent incident management

**T**raditional incident management often struggles to keep pace with the increasing volume and complexity of IT incidents. Its reliance on manual processes results in processes that are slow, error-prone, and difficult to scale. AIOps provides a transformative solution by shifting incident management from a reactive, manual approach to a proactive, data-driven strategy that considerably saves the time and resources spent on incident resolution.

Advanced AI and ML algorithms can intelligently analyze incoming incidents, discerning the issue description, resolution status, and reopen status. This advanced analysis delivers tailored insights to IT managers, empowering them to streamline and optimize their incident management processes. Furthermore, AI-powered analytics reduces the time and effort spent on incident triaging, minimizing delays and ensuring swift attention to critical gaps, ultimately improving response times and overall incident resolution efficiency.

Consider a typical IT service desk within a large enterprise grappling with a significant daily influx of incidents. When the IT team depends solely on traditional methods, it can result in bottlenecks and potential escalations. These delays in resolving incidents can also contribute to an expanding backlog of unresolved tickets, as depicted in the analysis below.



The analysis tracks the average incident resolution time on a monthly basis, enabling the monitoring of performance trends throughout the year and providing a comprehensive view of a service desk's incident resolution performance over time. The visualization highlights periods where technicians struggle to resolve tickets efficiently, resulting in substantial ticket backlogs.

AIOps-powered automated anomaly detection identifies periods with significant deviations in average resolution time and backlogs, indicating potential declines in incident resolution performance.

IT teams can then delve deeper into these identified anomalies to understand the underlying causes and gain actionable insights for improvement. Traditionally, this triage and corrective action process requires service desk managers to spend considerable time analyzing various metrics and trends to pinpoint inefficiencies and develop effective strategies. However, with **Spotlight, ManageEngine Analytics Plus' contextual decision intelligence engine**, this is achieved in a few minutes.

For example, the analysis reveals that December exhibits anomalously high values for both average resolution time and the number of unresolved tickets.

Spotlight automatically monitors and analyzes the service desk data for December, identifies the key factors contributing to the unusually high resolution times, and provides data-driven, actionable recommendations to address them, as shown below. What once required days of meticulous monitoring and expert analysis is now delivered within minutes. It can automatically categorize these factors or events, and dynamically assign a priority based on crucial factors such as business impact, SLAs, and user criticality. This speed and precision in identifying and addressing root causes translate directly into cost savings by reducing downtime and the associated financial losses.

The screenshot displays the 'Spotlight' interface with four recommendations:

- Critical** (30 mins ago): **There has been a significant increase in OS update-related incidents over the last month.** Consider allocating additional technicians and providing specialized training to the technicians handling OS issues. Investigate potential problems with the OS update deployment process.
- Critical** (24 mins ago): **20% of technicians are responsible for 60% of the unresolved tickets in December.** Review ticket assignment and workload distribution. Reallocate tickets from overloaded technicians David and Sarah to Jim and Toby to improve overall resolution efficiency.
- High** (10 mins ago): **18% of tickets have been reopened due to unresolved issues or incomplete fixes.** Analyze these reopened tickets to identify common issues. Provide additional training to technicians on ensuring a complete resolution before closing a ticket.
- High** (15 mins ago): **The average resolution time for high-priority incidents has increased by 30% in December, breaching SLAs.** Review the handling process for high-priority incidents. Implement automated escalation rules and ensure that these incidents receive immediate attention from senior technicians.

The above snippet of Spotlight's recommendations highlights overall performance gaps identified from service desk data and pinpoints areas requiring attention. Spotlight further dissects the underlying causes of these insights, categorizes them based on criticality, and provides specific, actionable recommendations for improvement.

By integrating advanced AIOps-driven analytics capabilities, such as automated anomaly detection and decision intelligence, IT teams gain a powerful ally for achieving intelligent incident management. This empowers IT organizations to effectively identify and address resolution gaps, leading to enhanced incident resolution efficiency, reduced operational costs, and improved customer satisfaction. The reduction in operational costs stems from decreased downtime, lower labor expenses, and the ability to prevent future incidents through proactive analysis.

03

## Detection of insider threats from privileged accounts

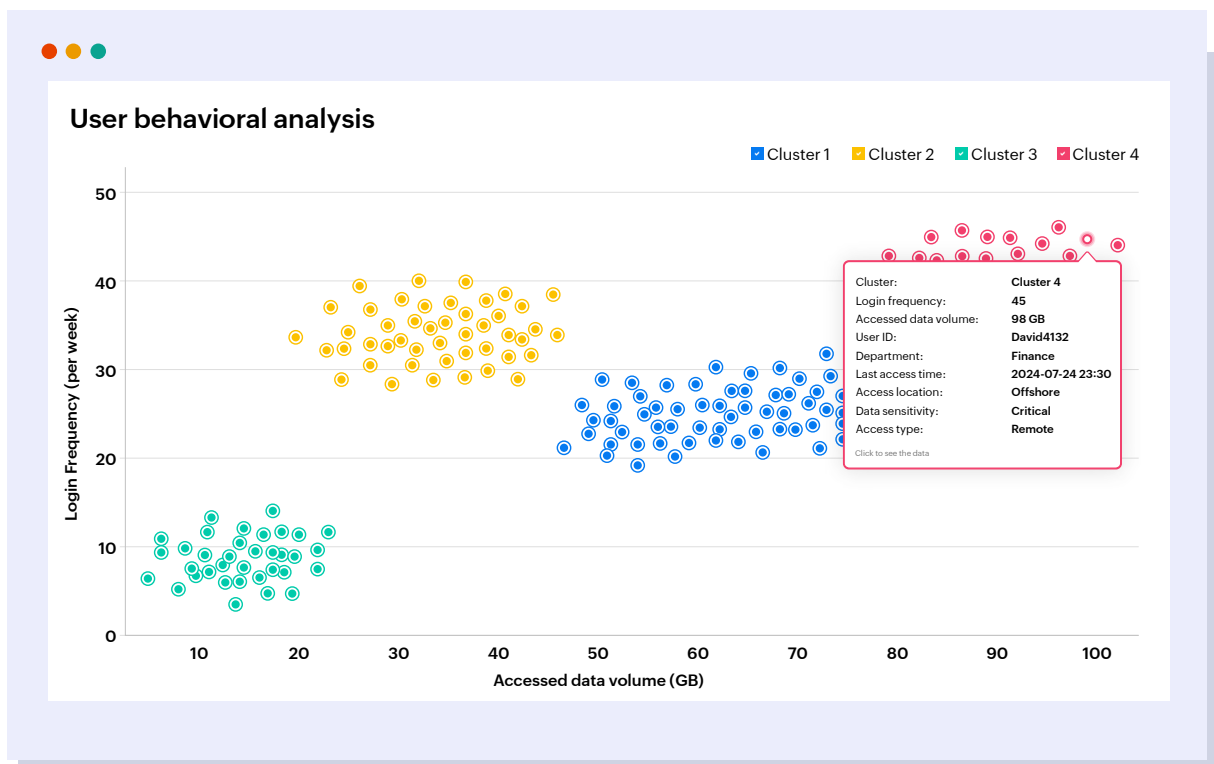
Often, the most significant threats to modern IT infrastructure don't originate from external adversaries but from within the organization. Insider threats, carried out by employees, contractors, or other trusted individuals, pose an insidious challenge. These threats are difficult to detect because they involve individuals with legitimate or privileged access to sensitive systems and data. The potential financial damage from insider threats, including data breaches, intellectual property theft, and regulatory fines, can be substantial, making effective detection a critical cost-saving measure.

Traditional security measures like firewalls, intrusion detection systems, and antivirus software, while crucial for external threats, lack visibility into the actions of those operating within the trusted network. The real challenge lies in sifting through the vast amounts of user activity data to identify subtle deviations—the early indicators of malicious intent—before they escalate into damaging security breaches. The longer these threats remain undetected, the greater the potential for financial loss and reputational damage, further increasing costs.

AIOps provides a powerful advantage in combating insider threats. Leveraging the power of advanced analytics, IT teams can meticulously track user data, particularly that of privileged users, to establish a baseline of normal behavior. By incorporating AIOps, particularly ML-driven cluster analysis, organizations can create digital fingerprints of typical behavior and detect anomalies indicative of legitimate users abusing their access.

Like a skilled detective meticulously sorting through clues, the algorithm groups users exhibiting similar behavioral patterns, forming distinct clusters of unique behavioral profiles. By continuously monitoring user activity and comparing it against these established clusters, anomalous actions that deviate from a user's normal behavior can be flagged as potential threats or indicators of compromised accounts, thereby highlighting potential future cybersecurity vulnerabilities.

With advanced ML-driven clustering capabilities infused with IT analytics, IT and security teams can uncover hidden correlations and extract meaningful signals of insider threats from the noise of everyday user activity. This reduces the time and resources spent on manual investigations and incident handling, leading to significant cost savings.



The visualization above categorizes users of an organization's critical financial application based on key activity indicators, such as the average volume of data accessed and their login frequency. The analysis effectively isolates users with similar activity patterns into four distinct clusters, each representing a unique behavioral profile:

- **Cluster 1:** This group comprises users with a greater system usage, indicated by moderately high data access. These are often analysts or researchers performing regular data-intensive tasks. While typically considered low risk, their activity should be monitored for any uncharacteristic spikes.
- **Cluster 2:** This cluster includes users who require frequent system access throughout the day but for less data-intensive tasks. It is often comprised of users like customer service representatives or sales staff. Any deviations in their data access patterns warrant close attention.

- **Cluster 3:** This group might consist of executives or managers who primarily access the application for audits and reviews. However, they can be considered higher risk due to their potentially unrestricted access to sensitive data. Any activity outside their established normal pattern should be treated as high risk.
- **Cluster 4:** This cluster represents users with erratic patterns characterized by highly variable data access and irregular login frequency. Their behavior deviates significantly from the norm and exhibits sudden, planned increases in login frequency and data access. These users are considered high risk, demanding immediate investigation and attention due to the elevated potential for malicious activity.

By segmenting users into such unique behavioral clusters, IT and security teams can swiftly identify individuals whose activity deviates significantly from the established norm. These clusters provide valuable context, enabling security analysts to understand the typical behavior of different user groups and prioritize their investigations effectively.

The insights derived from this analysis can be leveraged to implement targeted security measures, such as enhanced monitoring, stricter access control restrictions, and tailored security awareness training, to effectively mitigate the risk of insider threats and safeguard the organization's sensitive data. By proactively preventing insider breaches, organizations avoid the direct costs of data loss, legal liabilities, and reputational damage, as well as the indirect costs of lost productivity and customer trust.

# Strategic capacity planning and resource cost optimization

In today's era of efficiency, characterized by tightening budgets and ever-increasing demands for compute and storage resources, effective IT resource utilization is paramount for both optimal performance and cost efficiency. Inadequate capacity planning and uncontrolled spending can be exceptionally costly for businesses, leading to lost revenue, decreased productivity, and reputational damage.

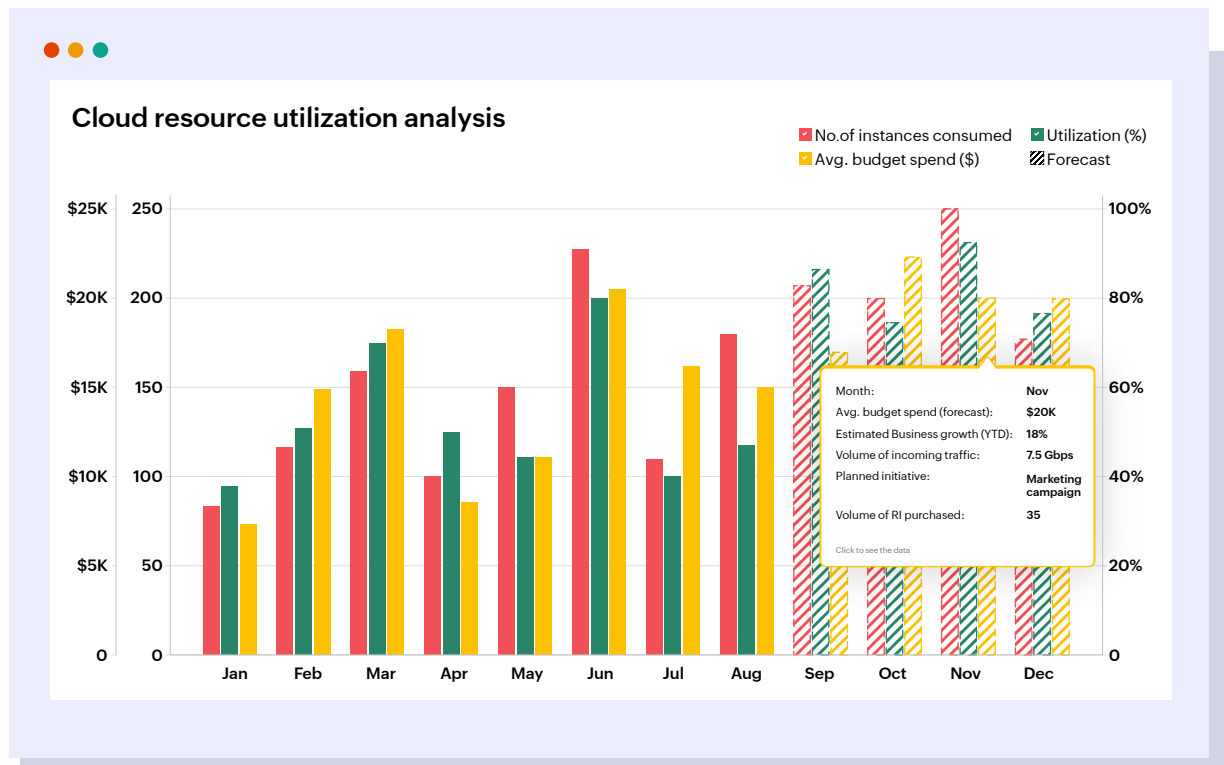
However, managing resource utilization and ensuring prudent spending across a modern, complex IT environment with distributed resources is a significant challenge.

AIOps delivers a powerful solution by enabling organizations to optimize capacity planning, streamline budgeting, and improve resource allocation through accurate forecasting of future needs and the identification of inefficiencies. It provides the essential visibility and insights required to optimize costs and ensure resources are used effectively.

IT analytics platforms like Analytics Plus provide advanced forecasting capabilities that are powered by AI and ML algorithms, enabling IT teams to predict future demand based on historical consumption and varying influential factors. While traditional forecasting engines rely solely on historical patterns, AIOps-powered forecasting also accounts for the influence of external factors on future resource consumption and expenditure. This technique, known as multivariate forecasting, aggregates spending data from diverse sources (cloud providers, on-premises infrastructure, etc.) to provide a comprehensive and accurate capacity plan for the future.



The analysis below, illustrating the trend of cloud resource utilization in an organization, demonstrates multivariate forecasting in action.

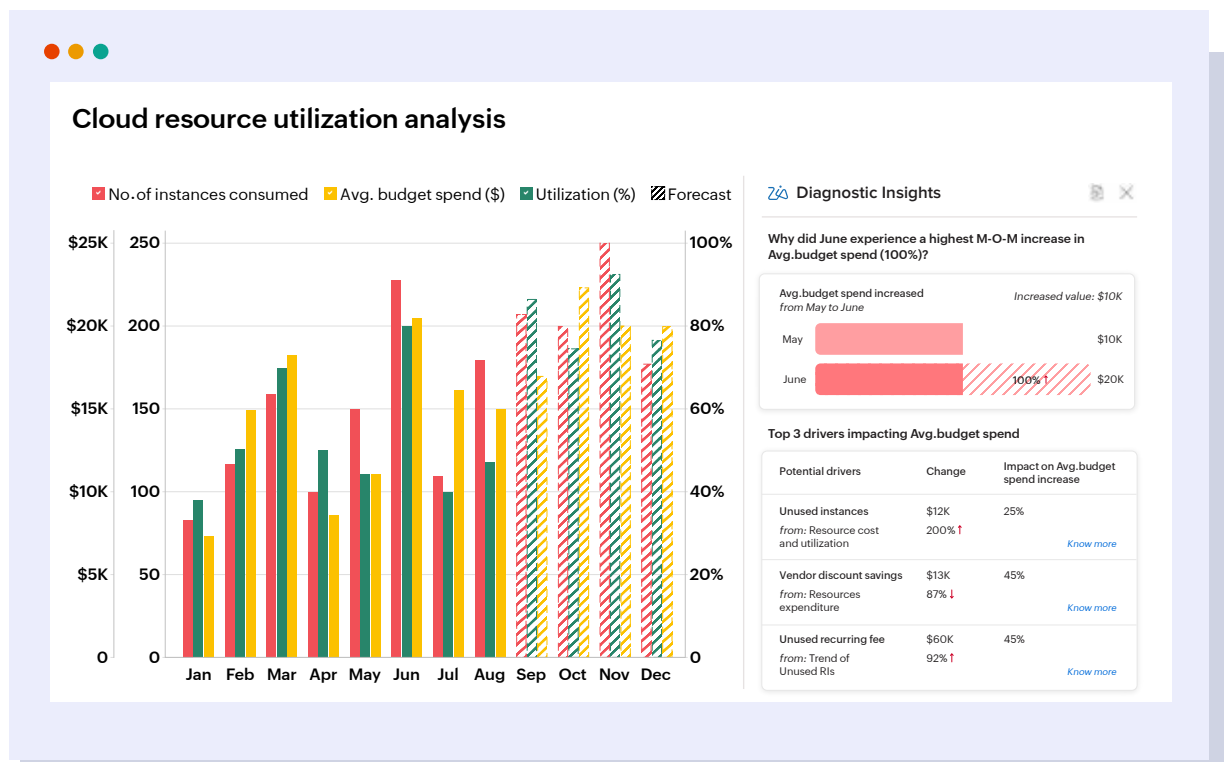


By considering past usage data alongside dynamic factors such as seasonal trends, ongoing marketing campaigns, and projected business growth, the analysis generates precise predictions for cloud resource spending and utilization.

Multivariate forecasting enables IT teams to dynamically scale resources up or down in real-time to align with actual demand, ensuring optimal performance without incurring unnecessary expenses. This proactive approach minimizes downtime caused by capacity shortages and prevents both the over-provisioning and under-utilization of valuable infrastructure resources, resulting in significant savings on resource costs and a positive impact on the bottom line.

However, this represents just one facet of the comprehensive benefits offered by AIOps-driven FinOps and capacity planning. An effective strategy is incomplete without identifying and mitigating the root causes that contribute to unusually high cloud resource expenditures.

Pinpointing the underlying reasons for overspending is crucial for preventing its recurrence.



The visualization above highlights AIOps-driven root cause analysis that analyzes cloud consumption data and identifies the top three factors contributing to anomalously high cloud resource spend overruns during the month of June.

This capability reveals the fundamental drivers behind the issue, such as unused instances, Reserved Instance (RI) utilization, and vendor pricing, and illustrates the interplay of these factors.

This empowers IT teams to implement strategies to improve resource utilization efficiently, including:

- **Identifying underutilized resources:** Analyze resource utilization data to pinpoint ineffective cloud and on-premises resource usage.
- **Rightsizing resources:** Discern optimal resource configurations based on actual usage patterns, thereby avoiding over-provisioning and reducing costs.
- **Optimizing resource allocation:** AIOps can track software license usage and identify opportunities to reduce licensing costs, such as reclaiming unused licenses or optimizing license allocation.
- **Vendor negotiations:** Facilitating better deals with vendors by identifying those offering more competitive prices and enabling the purchase of RIs and SIs based on accurately forecasted demand, thus reducing last-minute spending on on-demand resources.

## Conclusion

AIOps is fundamentally reshaping the landscape of IT operations and empowering organizations to move beyond the constraints of traditional, reactive IT management and embrace a new era of proactive decision intelligence. From preemptively identifying potential issues before they affect users to intelligently automating incident resolution and root cause analysis, AIOps empowers IT teams to operate more efficiently, reduce costs, and drive business value. As IT complexity grows, AIOps becomes essential for maintaining optimal performance and ITOps efficiency without burning a hole in your pocket.

# About

**ManageEngine Analytics Plus** is an IT analytics and decision intelligence solution designed to provide organizations with a unified view of their IT operations, correlate interdependencies and derive meaningful insights. It breaks down data silos by consolidating both on-premises and cloud infrastructure KPIs. Analytics Plus measures the efficiency of network operations, tracks the responsiveness and availability of business applications, evaluates technician performance, assesses the progress of processes and flags security anomalies. This comprehensive analysis is achieved by connecting to all IT software that forms the backbone of an IT infrastructure. These consolidated insights enable organizations to make data-driven decisions that enhance operational efficiency and drive business success.

For more information about Analytics Plus,  
visit: [www.manageengine.com/analytics-plus/](http://www.manageengine.com/analytics-plus/)

