

# 05 ANALYTICAL CAPABILITIES EVERY IT TEAM SHOULD ADOPT FOR SURVIVAL

Discover and deploy groundbreaking analytical advancements  
to transform IT outcomes

# Introduction

**T**he rapid evolution of technologies, driven considerably by AI frameworks, has introduced innovations and automations that have fundamentally transformed the way industries operate. Survival of the fittest has never rung more true. To remain competitive in this explosive environment, organizations must adapt to changing trends and adopt AI's diverse capabilities for operational sustainability and growth.

Analytics has proven to be a cornerstone of modern business strategies in this era, and a failure to deploy its growing capabilities can prove detrimental to organizations striving for improved outcomes and sustainable deliverables. This whitepaper highlights five significant AI-driven advancements in IT analytics that will play a pivotal role in ensuring organizations survive and thrive in the ever-evolving global market.

01

## Democratize strategic decision-making for improved efficiency

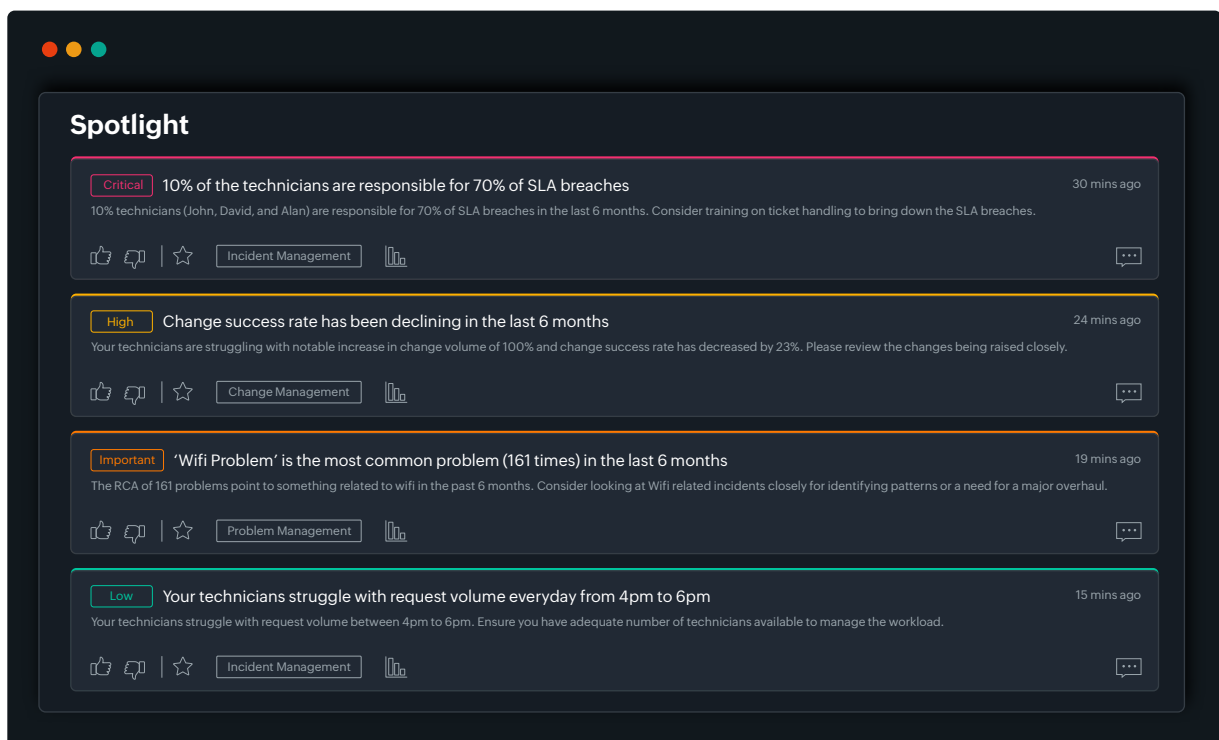
**O**rganizations turn to analytics to discover insights and implement timely decisions for greater efficiency and outcomes. Traditional analytics tools successfully democratized IT insights, eliminating the data barrier and effectively reducing the time taken to convert data into actionable insights.

While these insights can be used to fuel immediate action and preliminary corrective measures, there's still a vast gap between insights and powerful business strategies. This stems from the fact that decision-making involves significant human effort and expertise. Strategic decisions are therefore restricted to experts with domain know-how, inevitably delaying the time to strategic action and impacting operational efficiency.

To bridge this gap, organizations should adopt decision intelligence solutions to streamline, automate, and democratize contextual decision-making. Such tools meticulously monitor IT data, catch underlying inefficiencies and bottlenecks, and provide contextual strategies to remediate them.

Let's consider the example of a widespread service desk serving a global enterprise. Self-service portals, ML algorithms, and automation frameworks have cut down the effort involved in running successful large-scale service operations. On one hand, popular analytics tools have democratized the insights into these operations for wider consumption. On the other hand, even with self-service tools, it still takes time to arrive at data-backed decisions that improve service operations and SLAs.

Implementing timely corrective measures often involves service desk managers spending hours pouring over every metric and trend to catch inefficiencies and using these insights to create effective strategies. With Spotlight, ManageEngine Analytics Plus' contextual decision intelligence engine, this is achieved in a fraction of the time.



This contextual engine automatically monitors and analyzes a service desk's data, identifies hidden bottlenecks and inefficiencies, and lists data-driven recommendations to address them. What once required days of monitoring and expert analysis is now presented within minutes.

By adopting the advancements in decision intelligence capabilities, employees and leaders can equip themselves with the information needed to take timely action, expedite incident resolution, and halt breaches at their onset.


### Tip

Restricting analytics implementations to a visual analysis of daily operations via dashboards can be limiting. Today, context-aware decision intelligence platforms empower IT and business leaders to monitor operations and address inefficiencies in real time, seamlessly transforming data into actionable decisions in seconds.

## 02 Adopt a hassle-free approach to complex, tailored analysis

**IT** data is inherently complex; it's diverse, varied, and uniquely aligned with each organization's infrastructure and requirements. Standard analytical solutions are a good starting point, offering capabilities that generate valuable IT insights. However, these solutions often fall short for large-scale enterprises with mature analytics deployments and more intricate needs.

Despite advancements in self-service analytics, organizations inevitably face a threshold where standard tools can no longer meet their unique requirements. Tailored, complex analytical models become essential, accounting for an organization's specific usage patterns, infrastructure intricacies, market trends, and business objectives. Relying on traditional analytical tools to achieve this often creates limitations that hinder IT departments' growth potential.



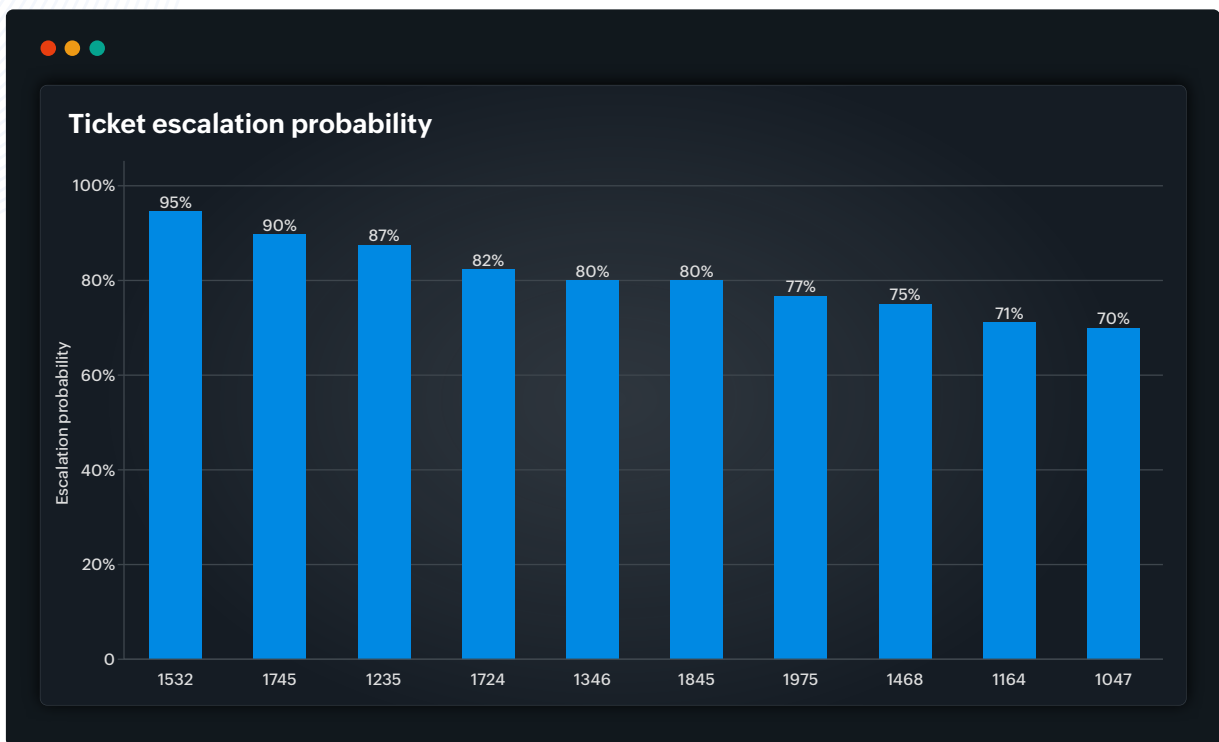
At this juncture, organizations often face two distinct paths: employ data experts to build custom analytical models from scratch or confine analytics efforts to the built-in capabilities of existing tools. While the first approach delivers accurate results, it significantly increases the time to insight. In contrast, the second approach degrades analytical accuracy, leaving organizations unable to meet their evolving demands.

No-code ML builders provide a transformative solution to this conundrum. They provide organizations with a code-free path to creating complex, custom analyses in seconds.

Let's consider an example of a service desk. For the service desk manager, escalations and SLA violations were recurring challenges. However, beyond optimizing overall resolution workflows, not much could be done to avoid ticket escalations.

No-code ML builders changed this narrative. The service manager can now create tailored escalation prediction models that assess the probability of a ticket being escalated. These models leverage historical data; simply pointing the platform to past records of escalated and overdue tickets allows it to generate an accurate ML model effortlessly.

With the generated model, the organization can seamlessly analyze current ticket data, generating accurate insights into each ticket's likelihood of escalation. Armed with this information, the service desk manager can implement precise, proactive measures to reduce escalations, streamline workflows, and improve overall service outcomes.



The entire process can be carried out in a matter of minutes, without requiring any complex code or data expertise. This powerful advancement empowers the IT industry to create tailored ML models for a variety of everyday requirements, forsaking the complexity and duration of traditional data science workflows.

### Tip

This functionality should be extended far beyond predicting service desk behavior. NOC teams can create custom analyses that anticipate infrastructure outages. Cybersecurity applications are also vast, ranging from accurately assigning threat severity levels to isolating endpoints with the highest likelihoods of a breach.

## 03 Automate root cause analysis for faster resolutions

Outages are a significant challenge for any organization, both for the technicians striving for their resolution and for the business leaders grappling with the financial and operational repercussions.

Root cause analysis is therefore a fundamental component of an IT technician's workflow, involving elaborate steps to identify the underlying issues that lead to inefficiencies, disruptions, and significant downtime. However, the process can be both time-consuming and cumbersome, particularly for organizations with disjointed departments and data storage systems. The longer this process takes, the more profound the impact on the organization, as evidenced by the following research:

An Oxford Economics report<sup>[1]</sup> estimated that downtime costs an average of

**\$540,000**

per hour and takes 75 days on average to recover from.

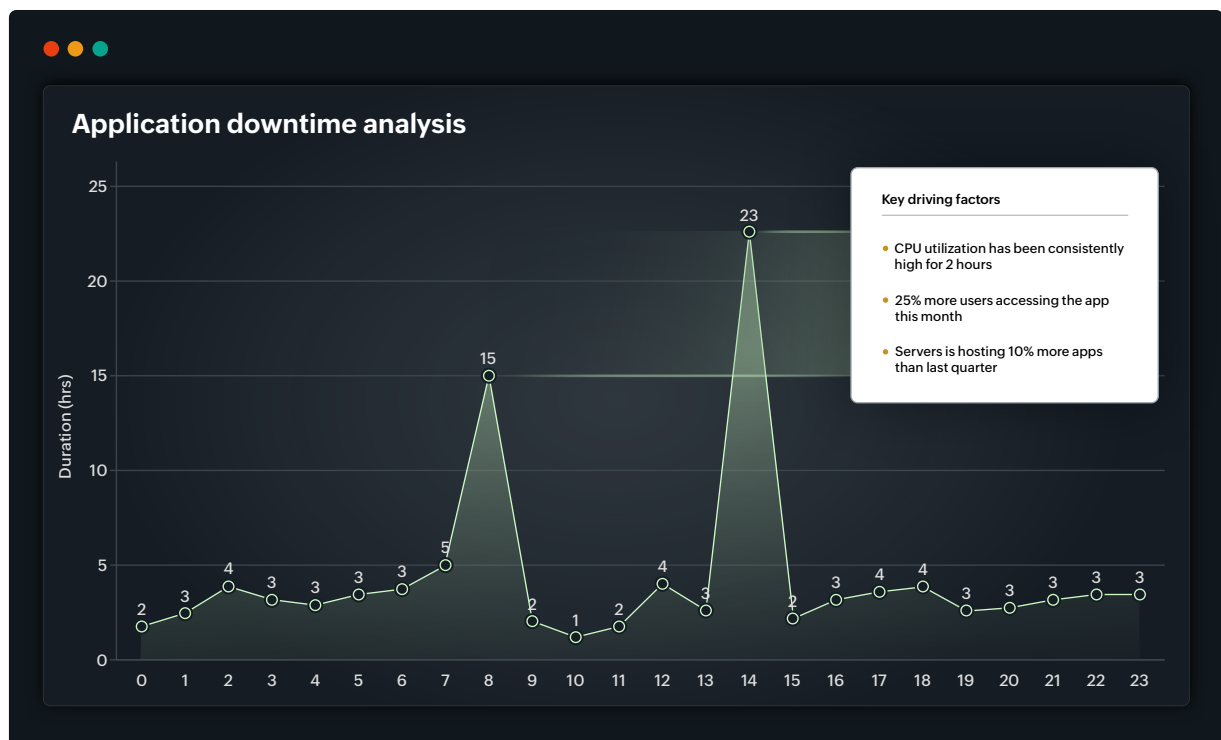
The recent CrowdStrike<sup>[2]</sup> outage resulted in an estimated overall loss of

**\$5.4 billion**

for United States companies, with Delta Air Lines alone incurring \$500 million over a five-day period.

Completely eliminating downtime may not be realistic, considering the hybrid nature of IT operations and the constant threat of security attacks. Instead, organizations should focus on strategies to minimize the duration of downtime. Two significant elements contribute to effective outage management and restoration: root cause analysis and efficient resolutions.

The good news is that advancements in IT analytics have resulted in tools and capabilities that accelerate root cause identification and help prevent outages before they escalate.



This analysis highlights key driver analysis, a cutting-edge advancement in root cause analysis that leverages automation to sift through an organization's complex data and identify the top three factors contributing to a specific trend. For instance, NOC teams can immediately uncover the elements responsible for an application's outage. What once demanded hours of careful analysis involving various techniques can be accomplished in a fraction of the time through advancements in AI technologies.

### Tip

Experts recommend extending this capability beyond the realm of outage resolutions and root cause analysis. Service desk managers can leverage this to evaluate the contribution of improvement strategies towards increases in SLA compliance. Similarly, security teams can utilize it to uncover underlying vulnerabilities responsible for anomalous spikes in monitoring KPIs.

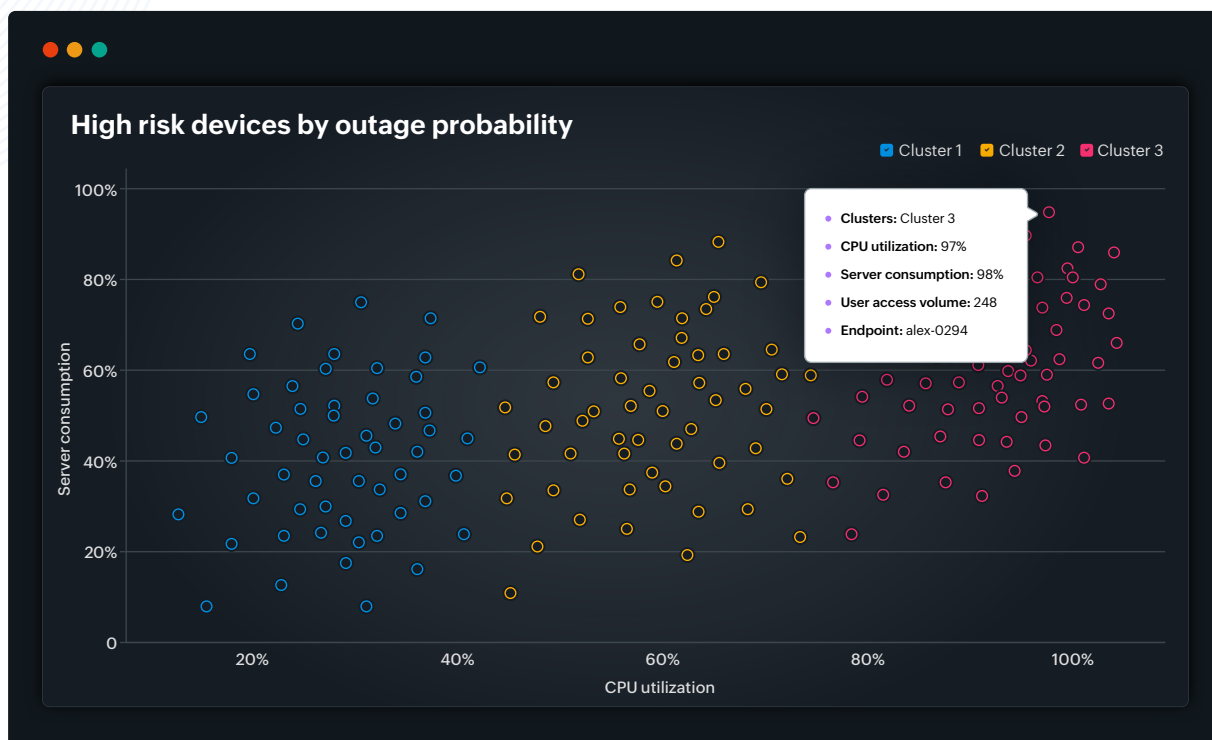
## 04 Deliver outcomes faster with clustering

Key driver analysis plays a pivotal role in automating the identification of an outage's root cause. However, the ball doesn't stop there. Far more can be accomplished through analytical advancements to streamline and expedite outage restoration processes.

Once a root cause has been identified, the logical next step is to isolate the affected entities. This is critical for facilitating remediation efforts and preventing threat progression in the event of a security breach. However, isolating compromised devices across a complex, hybrid infrastructure can be a time-consuming task, exacerbating the potential impact of the outage.

Traditionally, organizations rely on multiple legacy monitoring systems to hone in on affected resources, which proves to be a grueling process. Instead, employing frameworks that separate devices based on associated attributes gives organizations a valuable head start, enabling faster, more precise intervention.





The analysis above was created using powerful clustering algorithms that separate every resource by the configured indicators. Generic analytics tools categorize IT elements by a particular behavior or metric. However, this advancement allows IT leaders to separate elements based on a combination of metrics and KPIs, allowing for a more niche isolation of resources. In this case, the analysis has isolated every device with attributes that point to a potential outage, categorized by the outage probability. Now, NOC or security teams can effortlessly apply targeted fixes and patches to address operational and security inefficiencies.

By immediately isolating the affected IT entities, organizations can fast-track remediation efforts, streamline incident resolutions, improve patch management, and fortify their overall security posture.

## Tip

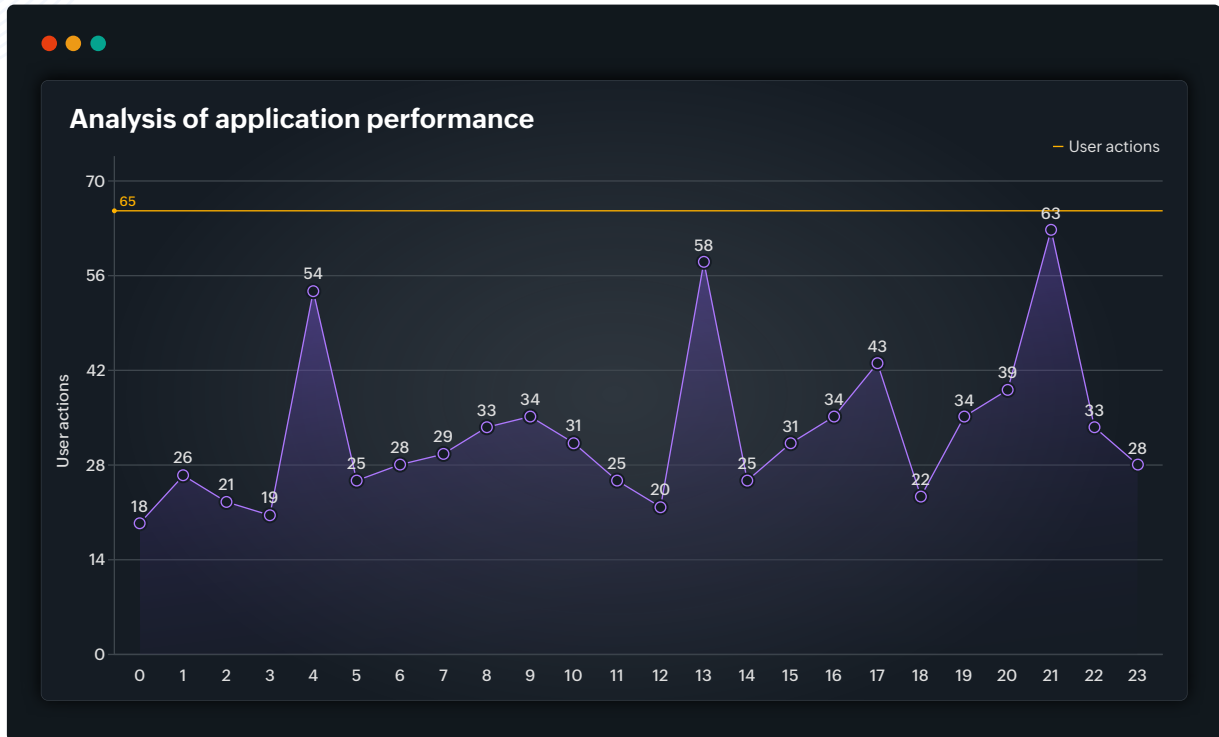
Similar to key driver analysis, clustering should be employed across multiple avenues to reap greater benefits. This includes categorizing hardware by the frequency and duration of failures; filtering out affected devices by indicators of compromise; categorizing service desk technicians by various proficiencies, like promptness, expertise, and the quality of issue resolution; and more.

## 05 **Flag abnormal IT events for timely intervention**

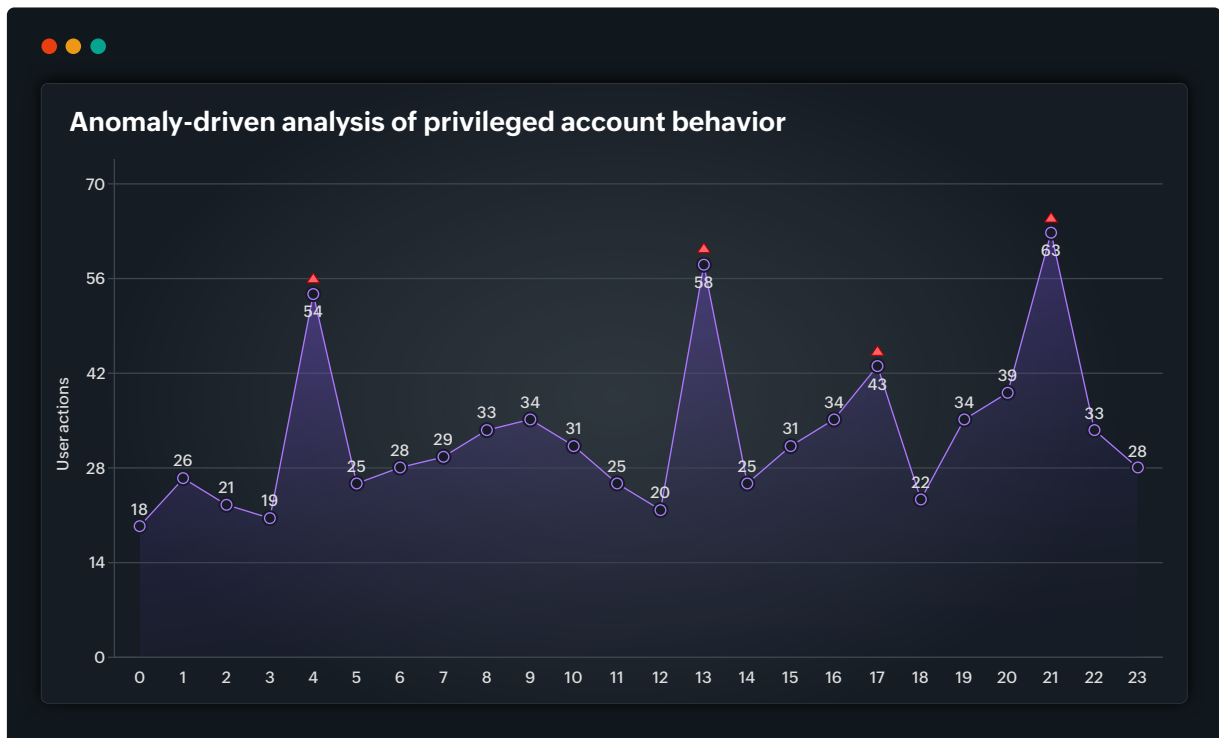
**E**very IT team worth its salt implements some variation of anomaly detection to catch deviations, both in IT operations and cybersecurity. Detection systems commonly rely on configured thresholds, and that's where they fall short. Static thresholds—and even the more recently adopted dynamic ones—fail to adapt to the unique and evolving usage patterns of an organization. The result? Alert fatigue. Technicians become inundated with excessive notifications, leading to them missing critical alerts that require immediate attention.

A better way forward is to forsake threshold configurations and implement automated anomaly detection. This advanced method identifies abnormal IT behavior based on the degree of variation from existing norms, offering a more adaptive solution. It effectively mitigates alert fatigue while ensuring timely, precise interventions.

For instance, consider a report designed to monitor privileged account activity during non-business hours. A traditional threshold-based system often proves ineffective, unable to distinguish between expected variations and actual anomalies. This can result in overlooked spikes in user activity that demand immediate scrutiny.



Graduating to an AI-powered configuration that evaluates deviations based on the degree of their variation from underlying trends enables the immediate detection of anomalies right at their onset.



This robust capability empowers security teams to identify suspicious activities as they arise while accommodating natural fluctuations in an organization's evolving landscape. By configuring alerts to notify key stakeholders of these detected anomalies, an organization gains a hands-free, proactive approach to anomaly detection. This advancement in anomaly detection serves as a powerful early-warning system, uncovering underlying inefficiencies and vulnerabilities before they escalate into large-scale issues.

### **Tip**

#### **Bestow analytics expertise on employees via GenAI**

While significant players introduced analytical assistants early on, recent vital advancements have brought GenAI to consumers' doorsteps. Analytical assistants that provide insights on command can now be integrated into existing applications and websites. This opens the door to powerful allies that deliver descriptive and visual insights to employees without mandating technical expertise. This move can effortlessly break the data barrier across an organization, expediting individual employees' outcomes and powering business growth.

## **Conclusion**

To adapt is to thrive. The analytical advancements outlined in this e-book provide organizations with a powerful edge in the technology race, enhancing outcomes, strengthening operations, and securing sustainable growth in an unpredictable market.

# 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 <https://www.manageengine.com/analytics-plus/>

**20+**  
years of IT  
management  
experience

**90+**  
products  
and free tools

**190+**  
countries  
served

**280K**  
customers  
across the world

## Reference

1. <https://www.oxfordeconomics.com/resource/the-hidden-costs-of-downtime-the-400b-problem-facing-the-global-200>
2. <https://nypost.com/2024/07/24/business/microsoft-to-take-hit-as-fortune-500-suffers-5-4b-in-crowdstrike-losses-study/>



© ManageEngine, a division of Zoho Corporation