Making Machine Learning Work for Your Mainframe

Enable early detection and actionable insights with multivariate analysis
Table of Contents

03 Executive Summary
04 Mainframe ITOM Today: Reactive, Overwhelmed, and Desperate for a Solution
05 Machine Learning for the Mainframe: Hype or Panacea?
06 Not All Machine Learning is the Same: Univariate vs. Multivariate
07 BMC AMI Ops Insight
08 Conclusion
Executive Summary

The rising complexity of modern IT environments extends all the way to the mainframe. As systems of engagement and systems of record become more tightly connected, it becomes harder for IT to ensure that internal and external customers can complete their tasks effectively. To avoid putting revenue and productivity at risk, IT teams need to become more proactive so they can detect, find, and fix problems before they impact service delivery. Artificial intelligence and machine learning offer exciting possibilities, but it’s often unclear to IT leaders where to begin or how best to move forward.

As IT seeks new ways to maintain quality amid rising complexity, IT operations management (ITOM) is an ideal starting point for leveraging Artificial Intelligence/Machine Learning (AI/ML). An AIOps approach blending applied data science, domain expertise, and multivariate analysis now makes it possible to reduce noise and false positives while detecting performance degradations and service disruptions. Actionable insights accelerate troubleshooting and guide resolution. As a result, mainframe teams can solve emerging problems even before they impact customers—for more reliable service, higher quality, and greater business value.
Imagine you’re on the mainframe ops team at major bank. It’s Monday morning, and you’re finally getting a chance to start mapping out a major transformation initiative. But suddenly an alert comes in—not from one of your mainframe monitors, but from Twitter. Customers are complaining about your bank’s ATMs, saying they’re running slowly or timing out entirely. Your monitors show higher CPU utilization than usual, but nothing that would raise an alarm. Finally you check the change management system and see that a new version of the ATM application was released over the weekend. You’ll need to do a table space reorganization in your database. It’s not a hard problem to solve, but your customers are already upset, your business looks bad, and there goes your productive Monday.

Whatever kind of organization you’re in, you can likely relate to this type of scenario. ITOM today is typically characterized by two de facto practices: monitoring by alarm, and managing by exception.

**Monitoring by alarm** is as bad as it sounds. All too often, problems that arise are missed by traditional monitors, with the first notifications arriving by phone, email, or social media posts from upset users. Even when system alerts do come, they report problems that have already begun affecting service—while failing to pinpoint the nature of the issue or offer guidance for resolution. By the time the problem has been diagnosed and fixed, the business is already dealing with angry customers. Inside the company, it’s the mainframe team that takes the blame.

**Managing by exception** helps explain why monitors miss so many problems: they’re configured to recognize things that have caused incidents in the past. If a problem hasn’t been seen before, there’s a good chance it won’t be detected the first time it happens until it’s too late. You might be able to avoid having the same problem a second time, but you’ll still experience the pain at least once.

Both monitoring by alarm and managing by exception reflect a fundamentally reactive approach to ITOM—one that forces mainframe teams to spend too much valuable time dealing with incidents and problems that are already affecting the business. Many of these problems could easily have been resolved well before they impacted service quality; while some issues manifest problems almost immediately, others linger in the background for weeks without being detected. By the time the phone rings or an alarm sounds, it’s too late for early resolution and the team has to start firefighting. Stuck in tactical mode, the team is unable to focus on more strategic work like planning for the future.

This situation would be challenging enough in a static environment, but in the modern data center, workloads, hardware, and software change continuously. Mainframe tools need constant adjustment to account for this change and complexity, and to cover new blind spots. It becomes harder and harder to understand new performance profiles, much less stay on top of thresholds and alarms. That’s especially true given the changing data center workforce, as experienced mainframe professionals...
retire and a new generation comes up to speed. Traditional mainframe tools have a steep learning curve, often requiring several months for a new hire to become fully productive.

To maintain service quality and shift from reactive firefighting to more strategic work, IT needs a way to detect problems earlier and resolve them more quickly.

- **Early detection** – To shorten the issue lifecycle, teams should be notified as soon as something in the environment isn’t normal—instead of waiting until problems begin—so they can resolve the issue before it impacts business services.

- **Actionable insights** – The mainframe team also needs information to help them troubleshoot, find, and fix the problem, even when its root cause is not immediately apparent in their monitors.

To address the challenges of a changing workforce, mainframe teams also need tools that can lower the learning curve for new hires from months or years to weeks.

Enter machine learning.

**Machine Learning for the Mainframe: Hype or Panacea?**

Across the industry, excitement has been building rapidly about the promise of analytics and machine learning. Within ITOM, a host of new products have been introduced promising artificial intelligence-based insights, machine learning, built-in domain expertise, predictive modelling, alert clustering, root cause analysis, learned remediation, and more—each claiming to be a cure-all for complex mainframe environments. In a recent report, 26 percent of CIOs surveyed by Gartner state that AI/machine learning is a game-changing technology.¹

At the same time, most of these CIOs have had reservations about actually adopting ML, with almost 80 percent confessing to a fear of the unknown.² This may be attributable at least in part to confusing and seemingly overlapping vendor strategies that make it difficult to know where to start, or even how to measure effectiveness once the technology is in place. The confusion is understandable; not all ML products are the same. Various solutions are based on different definitions of terms and different approaches to solving problems. They often target different problems, and provide different value. This lack of consensus can make clarity all too elusive for IT leaders.

To move forward successfully, IT needs a clear sense of the right use case, the right technologies, and the right solution to ensure full value from their ML initiative. Mainframe ops offers an ideal way forward. Modernizing and accelerating issue resolution is a clear challenge that can be addressed through a straightforward application of sophisticated, proven technologies, resulting in the clear business value of increasing uptime and improving MTTR.

¹ Gartner 2019 CIO Survey
² Gartner 2019 CIO Survey
Not All Machine Learning is the Same: Univariate vs. Multivariate

Machine learning comes in many variations. On a fundamental level, the underlying data analysis can be univariate, bivariate, or multivariate. As it sounds, this has to do with how many variables you’re looking at: one, two, or several. Which approach you take makes a profound difference in the effectiveness of the analysis.

**Univariate anomaly detection: the most basic form of data analysis**

Most approaches to ML-powered ITOM rely on univariate anomaly detection. These solutions look at one metric at a time, such as CPU times or log I/O, to find outliers. Alert clustering seeks to identify relationships among anomalies—but with a univariate approach, this analysis is performed only after each individual alert has already been triggered.

In addition, univariate anomaly detection is still threshold-based, meaning that alerts are triggered when a metric reaches a given point, rather than based on a deeper understanding of what’s happening in the system. These thresholds may be dynamic—for example, set differently at different times of day to reflect normal usage patterns—but they remain arbitrary. If a workload is introduced at an unusual time, a univariate threshold will perceive the resulting spike in utilization as a problem even when none exists—and trigger a dozen different alarms for the various metrics that exceed their arbitrary threshold.

While univariate anomaly detection can result in a flood of false positives, it can also fail to detect slow or progressive problems. In these cases, there may not be individual metrics that have gone out-of-band, but a set of related metrics has been changing in way that might signal a developing problem.

**Multivariate anomaly detection: sophisticated data science**

Multivariate anomaly detection goes beyond the one-dimensional limitations of univariate approaches to provide a fuller, deeper understanding of the mainframe environment. A multivariate solution looks at several metrics at a time, as a group, using domain expertise to ensure that the correlations among them are true—in other words, that a causation relationship between variables has been established. This is a key concept: just because two things happen at the same time, this doesn’t necessarily mean that one causes the other, or that there’s any relationship at all between the two. Without applying domain expertise to ascertain whether one outlier is actually causing another, an analysis can result in a spurious correlation, a finding that wrongly implies a cause and effect between two variables. The combination of data science with domain expertise provides confidence that multivariate metrics are true indicators.

Instead of looking narrowly at metrics on a threshold basis, multivariate anomaly detection considers how related metrics are moving as a group to see whether they indicate a growing problem. This results in fewer false positives, since several related metrics going out of band at the same time are a more accurate indication of a real problem than a single anomaly
BMC AMI Ops Insight

BMC AMI Ops Insight puts the power of ML to work for mainframe ITOM. Multivariate anomaly detection enables early detection to predict system impact issues before they create degradation and performance issues or unplanned outages. Mainframe teams see less noise and fewer false positive while detecting more real problems, faster—even without previous experience.

Along with early detection, BMC AMI Ops Insight provides actionable insights to accelerate mean time to repair (MTTR). By providing granular detail on the severity of the issue, its location, when it started, whether it’s getting better or worse, and the area where it has been projected (e.g. Contention, CPU, Throughput, Real Storage Virtual storage, Log I/O, or Workload), the solution speeds troubleshooting and resolution so service can be restored as quickly as possible.

Out-of-the-box data science helps overwhelmed teams leverage BMC AMI Ops Insight quickly and fully. Built-in domain expertise expedites the learning curve for new staff members; the solution knows which metrics to watch and how they correlate. Instead of having to select metrics and configure the solution, customers simply point it at their data lake and it can begin making predictions. The solution consumes deep and broad data continuously to learn and better support the complex mainframe environment it supports.

or multiple anomalies found in isolation. It also makes multivariate anomaly detection much more effective for detecting slow degradation, and for predicting future problems before they have a chance to impact service quality. As a result, the mainframe team can shift from reactive firefighting to proactive resolution and a more strategic approach to IT.
Conclusion

Given the business-critical role of the mainframe, IT can’t afford to let a reactive approach to issue resolution sacrifice service quality or divert the attention of the mainframe team from more strategic work. Fortunately, ITOM represents an ideal use case for machine learning. By using multivariate anomaly detection to find and fix problems more quickly, mainframe teams can deliver better day-to-day service for the business—and more strategic value moving forward.

For more information
To learn more visit bmc.com/bmc-ami-oi