This IDC Technology Spotlight provides an overview of the modern, cloud-based, AI/ML-driven system monitoring and analytics market and profiles CloudIQ, Dell Technologies' offering in this market.

AIOps-Based Monitoring and Analytics Tools Reduce Risk, Optimize Performance, and Ensure Security

September 2021

Written by: Tim Grieser, Research Vice President, Enterprise System Management Software, and Eric Sheppard, Research Vice President, Infrastructure Systems, Platforms, and Technologies Group

Introduction

IT organizations are facing enormous operational challenges that must be overcome to satisfy business objectives and meet end-user needs. They not only must meet requirements for availability, capacity, performance, and security but also must drive operational efficiency and control costs. Growth in the number of applications and workloads is generating increasing volumes of telemetry data, making it difficult to monitor, track, analyze, and optimize the performance and health of today's complex infrastructures across servers, storage, and networks. The demands of remote work and digital commerce mean that IT must support "always on" operations, with speed and at scale. Ensuring, delivering, and maintaining high-quality service levels in these dynamic and complex environments require intelligence to detect service anomalies, predict and prevent interruptions and outages, speed troubleshooting and repair when needed, and gain insights and recommendations to improve infrastructure performance.

Traditional approaches to optimizing performance and availability for infrastructure and applications are frequently based on tools that read and interpret telemetry data including logs, metrics, and traces; perform some simple analysis; and display graphical information on a series of dashboards for operations personnel to visually interpret and troubleshoot. Often such tools tend to be siloed, aimed at specific operational roles or specific infrastructure technologies. Many of the problem-solving capabilities of these tools come from operator experience and domain knowledge. As infrastructure and applications become more complex and operate at higher scale, with huge volumes of telemetry data, achieving successful outcomes with simple monitoring tools and multiple dashboards becomes increasingly difficult.

Applied knowledge and automation become necessities for successful operations, at scale, especially for digital applications and high-volume transactions. Artificial intelligence for IT operations (AIOps) solutions incorporate machine learning (ML) and predictive analytics technologies to improve and accelerate IT operations. Cloud-based AIOps solutions drive operational efficiency and agility, support positive user experiences, and contribute to successful business outcomes. These solutions can streamline and simplify IT tasks and automate specific IT processes, accelerating speed, efficiency, and agility by performing tasks faster and reducing the time spent on routine IT operations.

Benefits of Cloud-Based AIOps

AIOps technologies extend and automate capabilities for optimizing specific IT operations tasks such as reducing alert volumes, dynamic thresholding, anomaly detection, root cause determination, and automated remediation. Key benefits include the following:

» Improved performance and availability of critical business applications

» Reducing the time needed for problem detection, root cause analysis, and problem resolution

» Preventing potential outages and degradations through predictive analytics

» Optimizing storage capacity forecasting and planning

» Cost efficiencies achieved through time savings

Cloud-Based AIOps Departs from Traditional IT Monitoring

Today's enterprise infrastructure teams are dealing with a level of scale and complex interdependencies unlike that of any other time in the past. Organizations of all sizes are racing to place applications and infrastructure in a diverse set of deployment environments to meet the needs and expectations of their customers and employees as well as a complex set of business stakeholders and external partners. As such, enterprise infrastructure under management frequently includes systems that are deployed throughout the core, cloud, and edge spectrum of deployment locations. This has made it increasingly difficult for administrators to accurately monitor system performance, identify potential issues, and head off system slowdowns and failures. Locating shared resource bottlenecks and hardware failures and being able to redistribute application workloads to optimize performance have become, at best, arduous tasks.

Enterprise storage vendors have traditionally offered a remote connection into their systems to monitor them in real time, primarily to rapidly identify failures, perform real-time troubleshooting, and institute other remedial responses. This type of remote monitoring enabled faster resolution of problems when they occurred, but these systems have traditionally been reactive and had almost no visibility into the ecosystem in which the storage platform was running. The fact that these systems looked only at the storage often made it difficult to comprehensively understand what was causing an identified problem. Still, this approach represented an improvement over what had come before.

> Cloud-based AIOps represents a significant departure from the way vendors and IT teams interacted with their systems in the past and has become a competitive imperative for enterprise infrastructure providers.

Cloud-based AIOps represents a significant departure from the way vendors and IT teams interacted with their systems in the past and has become a competitive imperative for enterprise infrastructure providers. These relatively new tools use remote telemetry data — now standard in most hardware — and root cause analysis to act like the canary in the coal mine, sniffing out potential system issues before they become problems. AIOps enables proactive notification of issues and recommendations so that users can self-remediate issues and resolve them faster than the traditional vendor support process.

The idea behind a cloud-based AIOps platform transcends the original goals of traditional remote monitoring capabilities across several areas. Whereas the older remote monitoring systems either retained log data on the array itself or fed collected data into a private database behind a supplier's firewall, today's cloud-based AIOps tools store such data within secure cloud resources, usually owned and operated by the infrastructure vendor. This is an important distinction as the cloud makes it easy to expand the value of the platform as the amount of useful data grows. Suppliers, for example, can leverage AI/ML and other algorithms to automate monitoring and analytics at a scale and speed not possible just a few short years ago.

The three key features that distinguish cloud-based AIOps applications from traditional offerings are as follows:

» **Cloud-based application versus on-premises application.** Cloud-based applications offer immediate time to value for first-time users and continuous fast time to value for new features from suppliers because the host updates the application versus users hosting and updating releases on their premises. Cloud-based AIOps also enables the supplier to make new features, such as health checks with recommended remediation, instantly available for the entire installed base of systems, leaving no end user behind. The ability to collect and retain data in the supplier's secure cloud also makes it very easy and safe to share data with many constituents across the end users' IT organization and, with the end users' permission, among their suppliers' support staff.

» **Scope of monitoring and recommendations.** Cloud-based AIOps supports the ability to analyze and monitor granular system information and offer recommendations for remediation on a very large scale from infrastructure across all the user associations. Depending on the supplier, this will include information from capex and opex (as-a-service) infrastructure and various services in public clouds. Importantly, cloud-based AIOps is increasingly supporting a wide range of infrastructure technologies and moving toward a more holistic level of visibility to monitor critical interdependencies between systems (servers, storage, data protection, networking, converged systems) and between systems and the virtual machines that support application workloads.

» **Use of AI/ML.** Machine intelligence is required to analyze the vast and growing amount of system information, whose vastness and velocity are beyond human capacity. The ability to analyze this information using AI/ML algorithms helps uncover new correlations, create more accurate trend analysis that looks not only at longer periods but also at any given time period in much more detail, and improve identification of anomalies and the reach of predictive failure analytics. AI/ML also helps expand the types of metrics monitored that don't fit the classic definition of a "failure" but would otherwise impact a system's performance, utilization, availability, cybersecurity, and so on.

Hardware infrastructure suppliers may leverage incoming telemetry from all users' systems as an anonymous pool of big data to analyze fleetwide behavior and program the AIOps software to execute new health checks across the installed base to identify and notify customers whose systems exhibit the issues.

Considering Dell CloudIQ

As one of the largest suppliers of IT infrastructure in the world, Dell Technologies is an important player within the AIOps application market. CloudIQ is the company's cloud-based AIOps offering that leverages machine learning to provide a robust set of proactive monitoring and predictive analytics capabilities for a wide range of infrastructure. CloudIQ is designed to combine considerably large amounts of system telemetry with a suite of machine learning and other algorithms to provide near-real-time and forward-looking insights into customers' deployed Dell Technologies infrastructure.

CloudIQ is distinguished by the wide breadth of infrastructure systems that it supports, including Dell Technologies':

» **Servers —** PowerEdge

» **Storage —** PowerStore, PowerMax, PowerScale, PowerVault, Unity/Unity XT, XtremIO, and SC Series

» **Data protection —** PowerProtect DD, PowerProtect DD Virtual Edition (VE), and PowerProtect Data Manager

» **Hyperconverged infrastructure —** VxRail and PowerFlex

» **Converged infrastructure —** VxBlock

» **Ethernet networking —** PowerSwitch

» **Storage area networking —** Connectrix

CloudIQ's proactive monitoring and predictive analytics capabilities are also distinguished in terms of where a customer's infrastructure is deployed. Indeed, CloudIQ can support infrastructure deployed within datacenters, edge locations, disaster recovery sites, and colocation hosting facilities, as well as data protection in public clouds. CloudIQ is also flexible enough to support infrastructure that is purchased through traditional capex methods as well as more modern opex agreements such as Dell Technologies APEX Data Storage Services. Importantly, CloudIQ brings together these diverse set of supported environments, locations, and consumption models by providing a consolidated/unified portal as a single source of truth.

The many features and benefits of CloudIQ start with its ability to combine large amounts of real-time infrastructure telemetry with modern machine learning techniques, predictive analytics, and other advanced algorithms. Thus, CloudIQ can continuously monitor the overall health of a user's infrastructure, including the availability and high-availability configuration of a system's components, the capacity and performance of a system, data protection, and system and cybersecurity configurations. This creates a core foundation on top of which CloudIQ offers the following capabilities:

» **Proactive Health Scores.** CloudIQ presents a consolidated view of the near-real-time information related to the health of the infrastructure within its purview in the form of valuable health scores. These health scores — a composite of performance, capacity, components, configuration, and data protection status — provide administrators with an efficient overview of any issues within their infrastructure in a way that supports informed prioritization and rapid remediation.

» **Proactive Notifications and Recommendations.** CloudIQ proactively notifies operations teams of any issues the moment they surface and offers recommendations for rapid remediation. Administrators can customize how they receive notifications in a way that best aligns with their workflow and maintains optimal productivity.

» **Performance Analysis and Anomaly Detection.** CloudIQ tracks key performance indicators (KPIs) and uses its native machine learning to understand normal behavior and to identify incidents or anomalies. Visualizing these normal and anomalous KPIs over times series charts allows administrators to quickly troubleshoot unexpected performance issues and take the action needed to remediate.

» **Virtualization Monitoring and Workload Contention Analysis.** Integration with VMware provides virtual machine (VM) performance details, and this is visualized with end-to-end mapping and performance impact analysis across the data path: VM, ESXi host, datastore, network, and storage. Time correlation of the KPIs for each of the components across the path reveals probable root cause. In addition, from a storage perspective, CloudIQ identifies workloads that are competing for shared resources and need to be redistributed to maintain desired performance.

» **Capacity Prediction, Forecasting, and Anomaly Detection.** CloudIQ uses machine learning algorithms to predict future capacity status based on seasonality of usage. This helps drive critical awareness of where capacity utilization rates are likely to be, starting at a three-month window. Capacity utilization can also be forecast over selectable timelines to enable accurate, longer-term budget and workload allocation planning. CloudIQ also proactively monitors capacity for anomalies that can drive rapid capacity utilization increases so that administrators can take swift actions before applications run out of space to write data.

» **Integration with Third-Party Tools for Automation.** CloudIQ leverages Webhook and REST APIs for efficient communication with third-party applications and services such as ticketing systems or collaborative/communications applications. This allows CloudIQ notifications and data to be integrated into broader IT workflow and processes, further increasing productivity and the value of its insights and capabilities. Triggering service tickets and escalations with recommended actions for manual remediation or with an option to execute automated remediation is a common use case.

» **Infrastructure Cybersecurity.** CloudIQ continuously monitors infrastructure for security risks by comparing the configuration of resources against a preselected set of security policies. CloudIQ proactively sends notifications to users when a system deviates from a secure configuration and includes recommended actions to reestablish a secure state. Recommendations are based on industry security standards, such as NIST, and best practices for each system's hardware and operating system software/firmware releases.

Challenges/Opportunities

Because AIOps is a relatively new software category, there is a risk that IT organizations initially view offerings such as CloudIQ simply as traditional system monitoring tools hosted in the cloud without fully realizing just how modern they are. AIOps solutions provide an opportunity for many IT organizations to step away from the tradition of the siloed teams, processes, and tools that mire them.

Infrastructure and operations teams and leaders should look at not only what data is collected by cloud-based AIOps platforms but also how modern AI/ML can be used to improve system performance, capacity utilization, and availability and to lower costs. Management applications that automate security monitoring and integrate with a broader spectrum of IT operations should also be an important consideration. Those vendors best at this automation should also be the ones that are most adept at communicating the value they deliver with these platforms.

Conclusion

Cloud-based AIOps tools represent a rapidly evolving part of the IT infrastructure market. Today's IT operations teams are likely well aware of how time consuming and inefficient it can be to manage and monitor enterprisewide infrastructure when forced to work with siloed tools that are far too manual and rife with hidden risks. Today, most organizations find themselves straddling the past and future worlds of true AIOps. Many are aware of the new generation of cloud-based, AI/ML-driven management and monitoring tools but have yet to fully leverage available offerings.

With the support of a technology partner such as Dell Technologies, such companies are expected to increasingly migrate to modern AI/ML-powered tools like CloudIQ to support their broader move of enterprisewide infrastructure modernization and operational transformation toward more automation and higher degrees of autonomous operations. When viewed at a macro or market level, increased adoption of these tools is expected to drive new levels of improvements to critical IT KPIs, including the following:

- » Improved application performance and availability
- » Rapid problem resolution
- » Increased prevention of faults
- » Reduced downtime
- » Improved resource utilization
- » Improved planning for future infrastructure resource needs

Viewed at a vendor level, CloudIQ offers a compelling AIOps solution by providing intelligent, proactive insights and recommendations for healing, optimizing, and protecting IT infrastructure. CloudIQ is distinguished by its coverage of the full infrastructure technology stack, extending to infrastructure as a service and public cloud, awareness of health and cybersecurity, and the API hooks to integrate with broader IT processes and boost IT automation and efficiency.

About the Analysts

Eric Sheppard, Research Vice President, Infrastructure Systems, Platforms, and Technologies Group

Eric Sheppard is a Research Vice President within IDC's Enterprise Infrastructure Practice, covering research on enterprise servers and storage systems, enterprise storage software, converged systems, and hyperconverged infrastructure.

Tim Grieser, Research Vice President, Enterprise System Management Software

Tim Grieser is Research Vice President for Enterprise System Management Software. His coverage includes software and SaaS solutions for managing systems, applications, and IT operations across a wide variety of deployment models including on-premises, private, and public clouds.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.