

SEPTEMBER 2024

Taming IT Operational Complexity: The Role of AIOps in the On-premises, Cloud-native, and Multi-cloud Era

Simon Robinson, Principal Analyst; and Monya Keane, Senior Research Analyst

Abstract: Thanks to the increasing complexity and volume of observability data, IT organizations are facing challenges in managing and monitoring their environments. Dell Technologies is addressing this problem with artificial intelligence for IT operations (AIOps), integrating machine learning (ML) and AI techniques to enhance infrastructure and application monitoring. The solution simplifies, accelerates, and automates operations, reducing event noise into manageable incident reporting and root cause pinpointing, thereby streamlining incident management and improving operations.

Introduction

As organizations continue to evolve their digital business strategies in the context of an ever-more complex landscape, their demand for smoother, more secure IT operations; faster, more innovative application development; and faster resolution of issues is increasing.

However, IT organizations are seeing their observability platforms and practices increasingly overwhelmed by telemetry data that is proliferating out of control. This issue stems from observability tool sprawl combined with limited automation, orchestration, visibility, and insights. In response, many IT leaders are now deciding to bolster their observability programs with AIOps capabilities.

AIOps' machine learning, natural language processing models, and a plethora of other algorithms provide crucial analytical insights into the health of systems. AIOps can react to problems in real time, providing relevant information to engineers and developers. It can even suggest or carry out solutions to rectify identified issues. But observability tool sprawl has resulted in an explosion of AIOps capabilities, including many point products that focus only on specific parts of the IT environment. That situation compounds complexity.

To help these organizations, [Dell Technologies](#) is taking a holistic approach to AIOps. Its multipart strategy focuses on the overall environment, in a manner that spans infrastructure observability, application observability, and incident management. By integrating those three elements, Dell can provide insights that reduce the “noise,” thereby enabling IT operations staff to create a more proactive, actionable, collaborative, and automated environment capable of empowering a digital business.

AIOps Takes Observability and Incident Management to the Next Level

IT organizations need a range of observability tools and platforms to meet the demands of their ever-growing, increasingly complex IT environments. In a study by TechTarget's Enterprise Strategy Group, 78% of organizations said they currently use observability practices in their environments, and the remainder planned to implement them

in the coming year.¹ Although the focus of observability varies across organizations, two key priorities stand out: These organizations want insights about their applications and infrastructure to assist with root cause analysis (RCA) and related problem-solving, and they want real-time insights into the application/infrastructure to ensure they are meeting service-level agreements.

However, more than half of organizations are taking a point-solution approach to observability, with 56% having at least 11 separate tools to collect data. This is creating challenges for them. Seventy-two percent of the survey respondents said the number of monitoring/observability tools they use is adding complexity to the overall environment, with 69% noting that their volume of observability data was growing at a concerning rate. Growing data volumes greatly increase the noisiness of an environment, raising the risk of false-positive alerts and extending the time required for RCA.

Enter AIOps

To address these challenges, many IT organizations are looking to apply ML and other AI techniques to their application and infrastructure monitoring environments. Enterprise Strategy Group found that 80% of respondents believed that the introduction of more automation or more tools with integrated ML would deliver meaningful improvements to business operations. Accordingly, the market is experiencing a rapid uptake of artificial intelligence for IT operations—namely, using AI to simplify, accelerate, or automate IT operations, maintenance, and management.

In the context of an observability practice, AIOps ingests data from multiple layers of the IT stack and continuously analyzes it using AI techniques to identify and diagnose issues as well as automate remediation. In other words, AIOps turbocharges observability and enhances many observability-related tenets—everything from supporting day-to-day IT operations to bolstering security and improving customer experience. Organizations are flocking to AIOps, with 55% currently using it and another 19% putting programs into place and expecting to use it within 12 months.

The rapid rise of AIOps makes sense when one examines the significant returns it offers. Most organizations using AIOps see benefits such as:

- Spotting hidden dependencies.
- An ability to address configuration drift.
- Accelerated code changes.
- Reduced false positives and eliminating noise.
- Accelerated root cause identification.

Between one-third and one-half of organizations reported that the benefits they've experienced have been substantial, and more than 95% of organizations have experienced those benefits to at least some degree (see Figure 1).

Despite the multiple, substantial benefits, AIOps isn't necessarily a magic bullet. Room for improvement exists. The study found that less than half of respondents implementing AIOps (46%) had simplified their operations enough to allow them to scale their observability practices. Additionally, more than a quarter of respondents (27%) said implementing AIOps had actually increased complexity and slowed down the pace of scaling their observability practice.

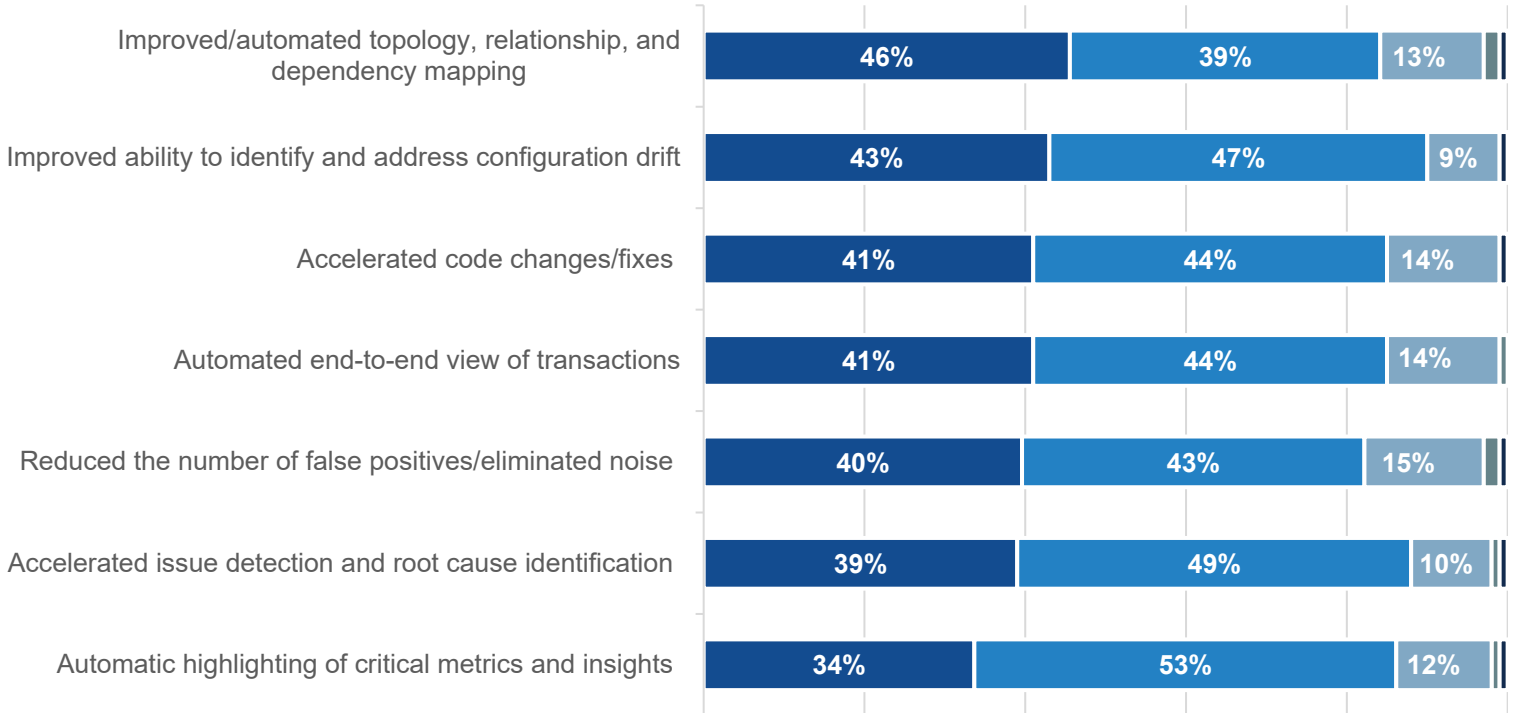
¹ Source: Enterprise Strategy Group Research Report, [Distributed Cloud Series: Observability and Demystifying AIOps](#), August 2023. All research in this showcase stems from this report.

It is likely that a combination of reasons is impeding some organizations from getting the most out of AIOps. One challenge is the relative immaturity of the technology. Another is that some of these technologies are too complex to deploy and manage, especially for organizations lacking sufficient in-house expertise. And, as mentioned, many AIOps observability products focus on individual silos, so they don't help IT operations teams to "connect the dots" comprehensively enough to resolve issues quickly across large, complex, diverse environments.

Figure 1. AIOps Benefits and the Extent of Realization

For each potential benefit of AIOps, please select the option that best describes your experience in your organization's monitoring/observability environment. (Percent of respondents, N=160)

- We have realized this benefit of AIOps, and the results have been substantial
- We have realized this benefit of AIOps
- We have realized this benefit of AIOps, but results vary
- We have not realized this benefit of AIOps



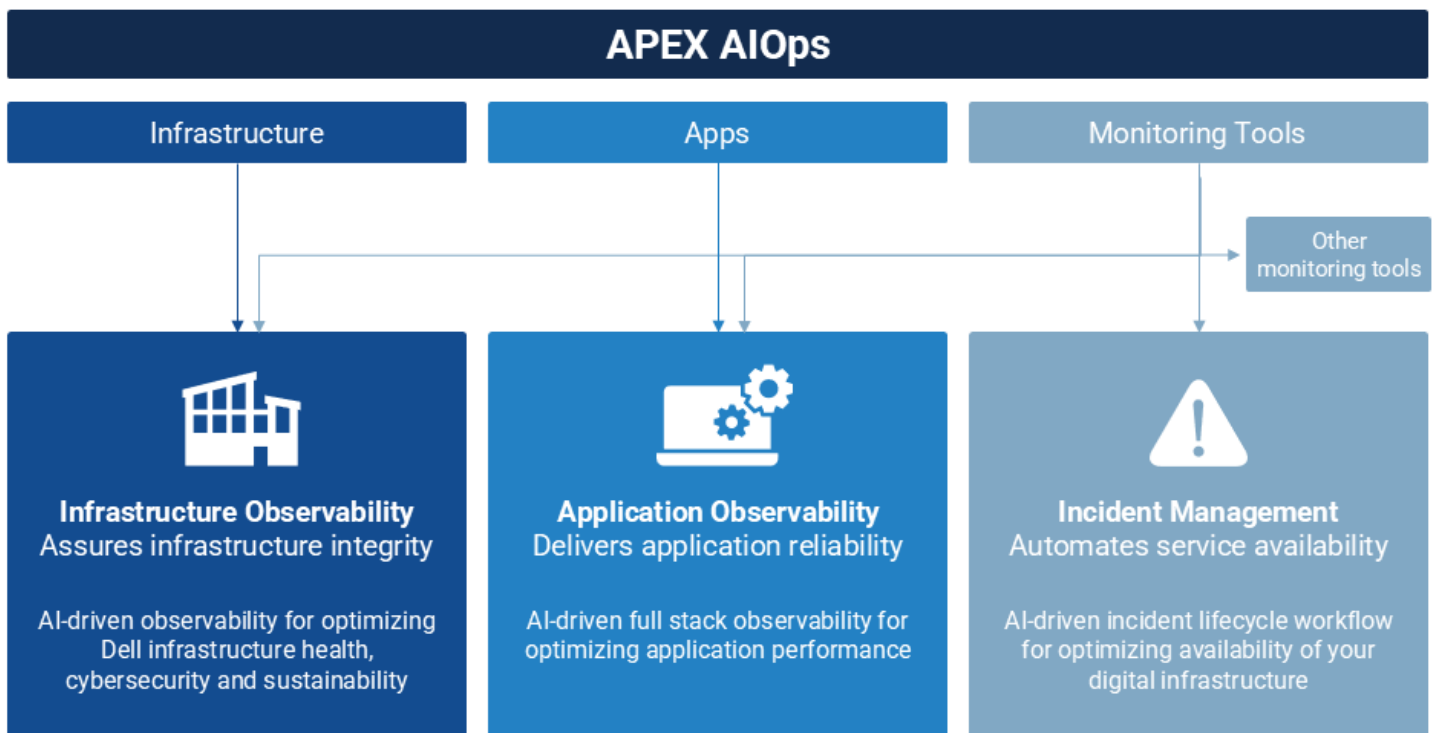
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Introducing Dell APEX AIOps—a Holistic, Integrated Approach to AIOps

Dell Technologies aims to tackle many of these issues, and more, head-on with Dell APEX AIOps, a new suite of offerings developed to help organizations tame IT complexity in their digital businesses. Dell has taken a holistic approach centering on a three-pronged strategy spanning an organization's entire digital business—from "ground to cloud" and "cloud to ground" across an entire infrastructure, application, and incident management domain.

This integrated approach (see Figure 2) simplifies an IT operations team's observability experience. It can provide insights more quickly than point-products can. It also caters to a broad range of organizations—not only those that use Dell's infrastructure solutions, but also those that don't.

Figure 2. Overview of Dell APEX AIOps



Source: Dell Technologies

Dell APEX AIOps Comprises Three Integrated Components

Dell designed its AIOps approach to align with three main capabilities. The following sections discuss each capability in detail.

Infrastructure Observability

Focused on assuring infrastructure integrity, Dell APEX AIOps Infrastructure Observability (formerly known as CloudIQ) is an AI-driven observability solution for optimizing infrastructure health, cybersecurity, and sustainability. It enables IT operations teams to know what's happening across their Dell infrastructure—including on-premises compute, networking, storage, hyperconverged infrastructure, data protection, and public cloud-based Dell infrastructure. It also predicts what will happen and what IT operations teams can do about it. Those insights enable system administrators, IT ops teams, and security ops teams to reduce risk, plan ahead, and improve productivity. Dell states that such organizations could resolve infrastructure issues up to 10x faster.

Dell Infrastructure Observability uses AI-driven workflows to provide capabilities such as:

- A detailed inventory of infrastructure components and their metadata.
- Health scores with recommendations and links for system managers to execute the recommendations.
- Capacity analytics, top consumption contributors, and capacity-full forecasting with anomaly detection.
- Performance analytics and maximum utilization forecasting with anomaly detection.
- Performance impact analyses and an end-to-end performance topology with probable root causes.
- Cybersecurity risk assessments and recommendations.
- Sustainability tracking and forecasting related to energy and emissions.

- Component failure prediction.
- Generative AI for queries and answers.
- Direct links to system UIs to execute recommendations.

A system could have any number of health issues related to components, performance, capacity, configuration, or data protection. Each issue affects the health score according to its severity value, driving IT staff to follow recommendations tied to issues that have the greatest health impact first.

APEX AIOps Infrastructure Observability gives an IT organization a common way to manage its infrastructure both on premises (core and edge) and virtualized in public clouds, simplifying enterprise-wide operations.

Application Observability

A Dell APEX AIOps Application Observability tool provides integration within the Infrastructure Observability tool's data and dashboards. This comprehensive capability supports system administrators and DevOps teams by automating full-stack visibility of application software components underlying Dell servers and storage as well as third-party servers. Full-stack visibility reduces risk, improves productivity with intelligent action, and, according to Dell, lowers mean time to restore services for application latency issues by up to 70%.

The Application Observability tool discovers and monitors more than 250 multivendor software technologies typically used to build and support applications. It spans on-premises, hybrid cloud, multi-cloud, and cloud-native application deployments. Notably, Dell APEX AIOps Application Observability uses AI-driven workflows to drive a long list of capabilities. These AI-driven workflows provide:

- Auto-discovery and instrumentation of application components.
- End-to-end call tracing at one-second intervals without sampling for performance monitoring.
- Trace metrics for application-level and microservice-level performance analytics.
- A full-stack topology of application and infrastructure components and the health status of each.
- A dynamic, real-time application microservices interdependency topology.
- Identification of the top microservices contributing to each application incident.
- Incident reports with a correlated sequence of events and issues.
- Root cause determinations.
- Recommended actions for remediation.
- Automated remediation through third-party tool integrations.

Dell also delivers an integrated reporting and management dashboard between the application and infrastructure observability layers. This dashboard enables IT operations teams to understand whether an issue is rooted in the Dell infrastructure or in the application, substantially simplifying triage and shortening the time to resolution.

For example, when the full stack topology finds that both infrastructure and application issues exist (displaying them in red), IT staff can directly launch an infrastructure health screen to see recommendations for resolving the issue and returning everything to a "green" status.

Conversely, the topology may show a green infrastructure status but red application status. In this case, the tool reveals which services are the biggest contributors to (i.e., root cause of) application latency. Staff can then follow recommendations, including automated workflows, to speed up resolution of the software layer issues.

Incident Management

The final component of the APEX AIOps portfolio is Incident Management, which enables network operations center (NOC) and site reliability engineering teams to automate service reliability. Incident Management is an outcome of Dell Technologies' 2023 acquisition of Moogsoft. In this portfolio, Dell is turbo-boosting the component's advanced, cloud-based AIOps capabilities.

Incident Management enables NOC and site reliability engineering teams, as well as the overall IT organization, to understand what is happening across an entire multivendor, multi-cloud digital infrastructure. It also automates ticketing and remediation.

Like the other two components, Incident Management uses AI-driven workflows to ingest events from an organization's ecosystem of multivendor observability tools. It filters and reduces those events into a smaller number of unique alerts, and then correlates those alerts into an even smaller number of unique incidents and root causes. Besides reducing the chaos of event noise, organizations using this tool have reported to Dell that it also reduces the number of customer-reported issues by as much as 93%.

APEX AIOps Incident Management automated workflow capabilities include:

- Data ingestion from popular, pre-integrated third-party monitoring tools, plus APIs, to create custom integrations.
- Event filtering, deduplication, and enrichment into unique alerts.
- Alert correlation according to actionable incidents.
- A situation room screen for collaborative, cross-team incident triage.
- A situation room notification to IT teams associated with each incident.
- A timeline of alerts and metrics associated with each incident.
- Root cause determination.
- Recommendations for manual and automated remediation.
- Pre-integration with third-party orchestration and automation tools for automated resolution and self-healing.
- Pre-integration with third-party IT service management and collaboration tools for notification service ticket creation and closure.

Significantly, this tool utilizes data from IT tools across an organization to provide a single pane of glass for IT staff to examine AI-driven root cause analyses of incidents. Such an effort would otherwise require hours or days of bridge calls to uncover the underlying cause of an issue.

For example, consider a situation in which end users are complaining about billing application outages, and IT specialists across the business are receiving a flow of critical event alerts from their various monitoring tools (e.g., Cisco Catalyst Center for Networks, Prometheus and Splunk for databases, Dell APEX AIOps Application Observability for application performance, and Dell APEX AIOps Infrastructure Observability for servers).

In such a situation, Incident Management uses a suite of AI algorithms to reduce all that event noise into a single incident, including timing to identify the root cause alert (versus symptomatic alerts) and recommendations to resolve it. Timing sequence and related metric data would reveal that the root cause in this case is a network switch that is dropping packets excessively; the database timeouts, application latency, and server performance anomalies were symptomatic side effects.

Conclusion

Organizations' environments are scaling up, becoming more distributed, and getting vastly more complex—not only from an infrastructure standpoint (core, edge, and cloud), but also in regard to the application layer and the data being ever more distributed.

These organizations are also on the receiving end of a tremendous amount of “noise” from their many different IT tools for monitoring and management, and that situation has worsened the already extreme complexity problem instead of improving it.

At this point, some IT environments are just so large and complex that it is effectively beyond human capacity to manage them efficiently without having AI in the mix. Taking note of this fact, Dell Technologies has stepped up to aid organizations by arming them with an AIOps-driven, common operating experience.

What Dell Technologies has unveiled is groundbreaking, and it is in part the result of Dell's highly savvy, high-profile investments in this space—including its acquisition of AIOps solution provider Moogsoft.

Overall, the solution offers real-time, end-to-end insights and recommendations without sampling, so no data is missed, in order to provide a truly accurate picture of a whole environment (covering both Dell and non-Dell technologies). It integrates the infrastructure view with the application layer view to create one comprehensive picture of the health of both elements together, which facilitates root cause determination. Moreover, it automates ticketing, remediation, and overall service reliability—a capability that, on a practical level, many organizations should find appealing.

Based on the trends that Enterprise Strategy Group is observing in the IT landscape right now, it appears that this is exactly the type of comprehensive AIOps solution that today's digital businesses urgently need.

©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.


Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

About Enterprise Strategy Group

TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

 contact@esg-global.com

 www.esg-global.com