

# APEX AIOps Incident Management

*AI-driven incident lifecycle workflow for optimizing digital infrastructure availability*

99% Event noise reduction<sup>1</sup>

50% Reduction in tickets<sup>1</sup>

93% Reduction in customer reported issues<sup>1</sup>

**Event Noise Reduction** reduces millions of raw events to thousands of unique alerts

**Alert Correlation** correlates thousands of alerts into single actionable incidents with probable root cause

**Real-Time Situation Insight** proactively detects business impact as incidents unfold

**Collaborative Team-based Workflow** streamlines communication across teams and tools using the Situation Room

**Algorithmic Knowledge** captures and codifies tribal knowledge from previous incidents for re-use, such as how past incidents were resolved

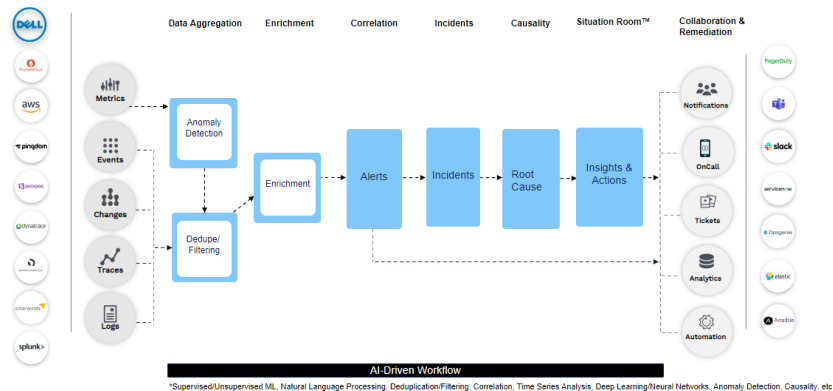
**ITSM and Runbook Integration** triggers tickets, escalation and remediation through integration with third-party IT tools

Ensuring availability of your digital infrastructure gets more difficult as your applications, data and compute, storage and network resources scale across data centers, edge locations and cloud. Events and alerts from monitoring tools across all technology domains make it difficult for IT Operations, DevOps and SRE to pinpoint root cause of incidents and inhibits resolution as your customers, employees and business suffer.

You need an AI-driven solution to tame the complexity.

APEX AIOps Incident Management, part of the APEX AIOps software-as-a-service, automates the availability of your digital infrastructure through automated, AI-driven incident lifecycle workflows.

It ingests data from all your multi-vendor IT tools and uses AI to reduce events and alert noise into single actionable incidents, identify probable root cause and mobilize the relevant staff to collaborate with precision and resolve incidents faster.



**Incident Management Automated Workflow:** Converts noise to actionable incidents and streamlines collaboration and remediation for faster time to resolution of service impacting issues.

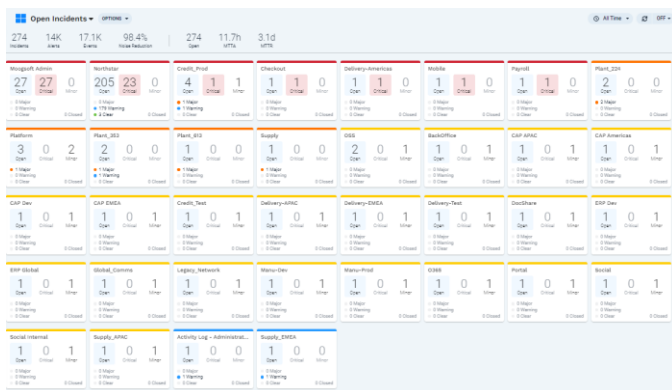
## Reduce alert noise and get actionable insights about service-impacting incidents

Incident Management is pre-integrated with more than 100 popular third-party IT monitoring and management tools and uses real-time machine learning (ML) and other AI algorithms to identify the relevance and relationships of operational data that it ingests. An easy-to-use interface lets you do additional integrations yourself.

As shown in the page one workflow diagram, Incident Management understands filters and discards incoming low-level events such as heartbeat signals and deduplicates the remaining consequential events such as a hardware component outage or application latency related events that require action. This reduces millions of events (as well as changes, traces, logs and anomalies) into thousands of unique, important alerts.

Next, an algorithmic correlation engine, which employs both unsupervised and supervised machine learning, infers relationships of alerts and their attributes for specific business impacts and incorporates them into a single incident.

Incidents are created in real-time as they continue to unfold in production, and algorithms cluster like incidents to further reduce noise.

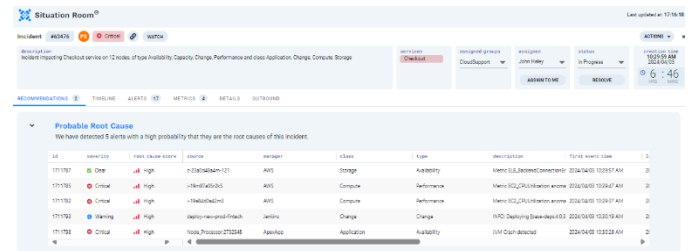


**Realtime Dashboard:** Custom dashboards provide immediate visibility into the current state of incidents across the enterprise. Dashboards can be easily customized to meet the unique needs of operation center, DevOps, SRE, server, storage, network or other teams, as well as line of business owners or other executives.

## Reduce time to pinpoint root cause

Causality algorithms identify changes in critical nodes in physical and logical topologies to assess and understand the impact of alerts. Supervised and unsupervised ML analyzes the patterns, previous incidents and timelines, proximity and linguistic aspects of alerts and changes to identify the most likely cause of each incident.

Probable root cause identifies key alerts as the root cause rather than requiring users to analyze potentially hundreds of alerts.



**Probable Root Cause:** Based on the trained model, the algorithm will display one or more alerts associated with the incident as the probable root cause to accelerate the remediation process.

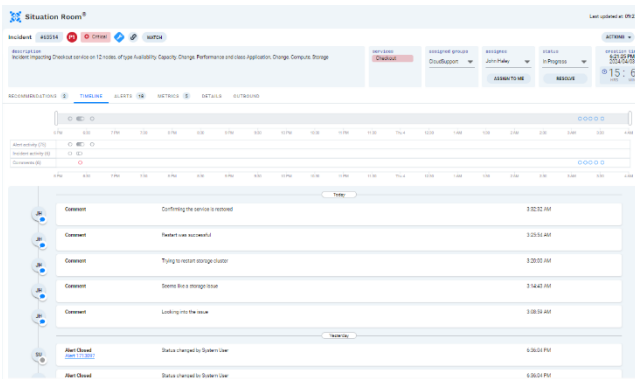
## Eliminate silos, improve collaboration and accelerate resolution

The heart of Incident Management is a collaborative-based workflow that automatically infers from an incident the relevant team to notify and directs them to the Situation Room. This is a virtual room for subject matter experts and other stakeholders to collaborate and efficiently resolve incidents by examining the incident, the probable root cause and the timeline and details of alerts.

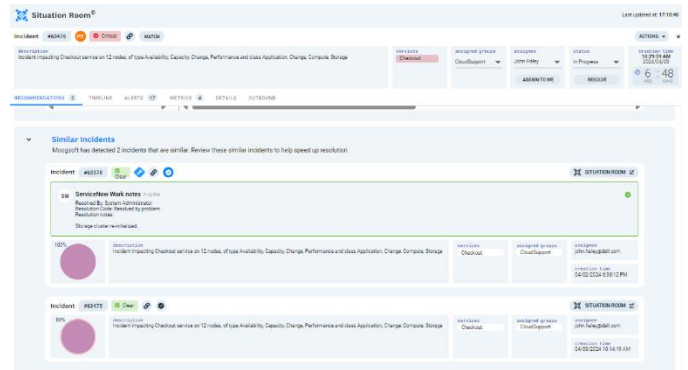
Algorithms compare current and past incidents. By assigning each incident a similarity percentage, teams can view and follow advice for remediation of similar, archived incidents. Teams can also identify recurring problems, as algorithms provide the insight needed to prevent damaging effects to business services before they occur.



**Time Series Metrics:** For deep insights, anomalies associated with each metric are displayed bottom-up, from the probable cause alert to cascading symptomatic alerts.



**Timelines and Details:** Additional insights are provided in a timeline of team member comments, actions taken, outcomes, assignment changes and more.



**Similar Incidents and Recommendations:** Historical, similar incidents as well as their resolving steps are displayed for each new incident. These resolving steps can be applied manually or programmatically using the API to remediate the issue causing the incident.

## Automate ITSM, escalation and incident resolution

APEX AIOPs Incident Management is pre-integrated with many popular ITSM tools (e.g., ServiceNow, Remedy, Jira) to initiate actionable service tickets, communication tools (e.g., PagerDuty, Slack, Microsoft Teams) for notification and to escalate action, and trigger automation tools (e.g., Ansible, Terraform) to automate corrective actions.

Remediation can be automated or manual if ongoing approval is required.

Learn more at [www.dell.com/apex-aiops](http://www.dell.com/apex-aiops)



Read [APEX AIOPs Product Briefs](#)



See [APEX AIOPs Demo](#)



Contact a Dell Expert



Join the conversation with [#DellAPEX](#) [#AIOPs](#)

<sup>1</sup>Customer Research, Moogsoft, 2024. Actual results may vary.