Drive down service outages with ITOM Health AIOps

The IT challenge

In today's digital world, businesses depend on software-based services to engage customers, automate processes, drive innovation, and unlock business insights. IT is responsible for delivering these mission-critical services and needs to ensure that they are always available and responsive. Otherwise, the financial and reputational impact can be devastating.

However, this is an enormous challenge. Many IT organizations continue to operate in silos, using multiple tools to monitor the health of individual domains, such as cloud and serverless infrastructure, networks, storage, and more. This leaves IT drowning in disconnected, redundant data, with a single issue often creating thousands of events. And, many events are just noise—they have no business or service impact.

IT staff must manually filter and correlate this deluge of event data—and, when they do finally get to the bottom of a service issue, there's no easy, automated way to remediate it. The result? Lengthy service outages, escalating IT costs, and mounting financial and competitive damage.

The ServiceNow solution

ServiceNow® ITOM Health uses the power of AIOps to turn this tidal wave of events into a trickle of actionable alerts—cutting through the noise, pinpointing service issues, and helping you to rapidly identify and remediate the root cause. Unlike legacy event management systems, which are static and rule based, ITOM Health applies machine learning and advanced analytics to correlate events, adapting automatically to rapidly evolving virtualized and cloud environments.

ITOM Health includes the following features:

- **Event Management** consolidates data from your monitoring tools, intelligently normalizing, deduplicating, filtering, and correlating events to generate meaningful alerts attached to corresponding CIs in the ServiceNow CMDB. This reduces event noise by up to 99%. Event management then shows you the service impact of these alerts— which services are affected and how badly—and it also lets you automate remedial actions.
- **Operational Intelligence** alerts you to anomalous behavior in your IT environment— potential service issues that are not necessarily captured by incoming events. It does this by using AIOps to automatically model normal behavior, eliminating the need to manually set and manage vast numbers of monitoring thresholds.

Together, these features help you to detect, diagnose, and remediate service issues far more quickly and accurately, dramatically reducing MTTR and increasing service quality.

Integrate with your existing monitoring tools

The Event Management feature includes out-of-the-box connectors to a wide range of monitoring tools, and you can integrate it with other event sources via custom REST, SNMP, JavaScript, and email connectors. Connectors developed by third parties are also available in the ServiceNow Store.

Intelligent, adaptive correlation

Event Management uses machine learning to identify temporal and topological patterns in your historical alert data. It then uses these patterns to correlate new alerts in real time, identifying groups of alerts that are caused by the same underlying issue. Instead of just seeing individual symptoms, you now know how these symptoms are related. You can also provide feedback on the usefulness of these groups, and you can even add or delete alerts. Event Management then uses this information to automatically modify its future alert grouping behavior.

BENEFITS

Improve service availability and reduce MTTR with AIOps

Leverage machine learning and automation to reduce event noise, transform events into actionable alerts, pinpoint service issues, identify likely root causes, and automate remediation. Measure service performance and identify anomalies that could lead to service outages or degradations.

Break down infrastructure silos

Consolidate events from multiple monitoring tools using a wide range of out-of-the-box connectors, easily create custom REST, JavaScript, SNMP, and email connectors, and leverage connectors built by third parties.

Leverage the combined power of ITOM and ITSM

Accelerate issue resolution with relevant, contextual change, problem, and incident data.

Increase productivity

Free up IT staff from time-consuming and error-prone tasks, including manually correlating events, creating and maintaining event rules, and setting and managing metric thresholds.

Deliver an intuitive user experience

See and prioritize service issues at a glance, seamlessly drill down to the underlying root cause, instantly identify CIs with similar issues, and resolve alerts using a single, integrated pane of glass.

Instantly see service impact

Event Management works seamlessly with ServiceNow® ITOM Visibility's Service Mapping feature, correlating alerts to identify impacted services. It then assesses the combined impact of these alerts on the service, displaying the results on an Event Management dashboard. This dashboard represents each service as a color-coded, resizable tile. This makes it easy to visually prioritize service issues based on issue criticality and service importance. Selecting a tile displays a list of alerts affecting that service, while selecting an alert highlights all of the services affected by that alert—allowing you to instantly see when issues with different services are related.
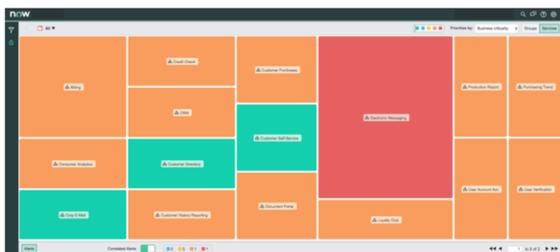
Event Management dashboard

Quickly diagnose service issues

Using the Event Management dashboard, you can instantly drill down into interactive service maps. Each service map shows all of the CIs that support the service, along with their upstream and downstream dependencies. CIs with alerts are highlighted, making it easy to see which CIs are experiencing symptoms. Automated root-cause analysis dramatically reduces resolution times by showing you the most probable cause of the service issue, including giving you confidence scores for individual CIs. And, because alerts are bound to CIs, you can also pull up IT Service Management data such as detected changes, planned changes, and incidents—giving you operational context to resolve issues even faster.
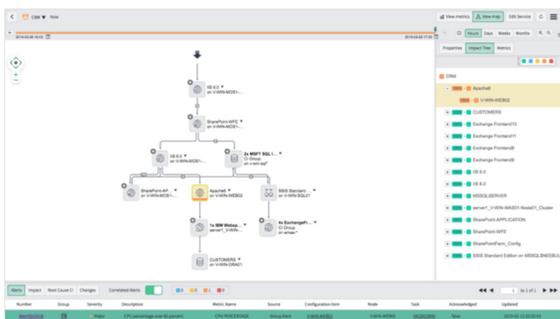

Interactive service maps

Accelerate resolution with Alert Intelligence

Alert Intelligence simplifies alert resolution by giving you a single pane of glass where you can see all of the critical information you

need to address an alert, such as the alert description, affected CI, severity, impacted services, and a timeline of secondary related alerts. It also provides Alert Insights, using machine learning to identify repeated alerts, similar past alerts and incidents, and relevant knowledgebase articles to help with root-cause analysis.
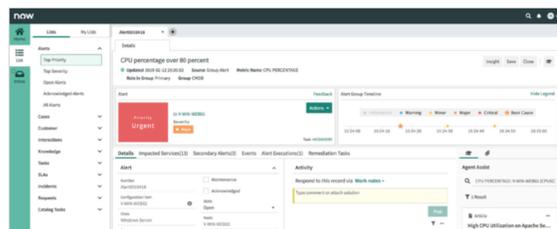

Alert Intelligence

Detect anomalous CI behavior with Operational Intelligence

ITOM Health's Operational Intelligence feature uses machine learning to analyze raw operational metrics, automatically determining normal behavior thresholds. It then detects and scores anomalies relative to these thresholds, with high scores indicating that a CI may be at risk of causing a service outage. Qualified anomalies result in alerts, which appear alongside other alerts in the Event Management dashboard and in alert intelligence. This allows you to detect issues that may not be captured by events and avoids the need to continually adjust thousands of thresholds in your monitoring tools.

Operational Intelligence also provides an anomaly heat map that shows you the CIs with the highest anomaly scores for a time period. You can drill down into each CI to see color-coded anomaly scores for each of its metrics, making it easy to identify problem areas at a glance.
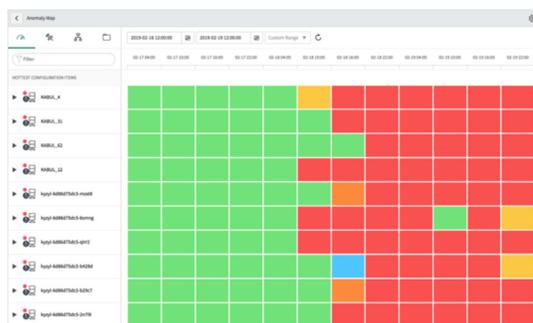
Anomaly map

Automatically remediate service issues

You can configure Event Management to respond automatically to alerts, helping you to resolve service issues faster. For example, you can use Flow Designer to create sets of remediation actions, such as retrieving log files, freeing disk space, restarting a service, or attaching a knowledgebase article to the alert. These actions are triggered when an alert meets specific criteria that you define. You can also automatically trigger tasks such as creating incidents, change requests, security incidents, field service work orders, or even customer service cases.

servicenow.