servicenow

Service health with AIOps from ServiceNow

Why traditional event management approaches fail—and how ServiceNow delivers

START

servicenow

Introduction

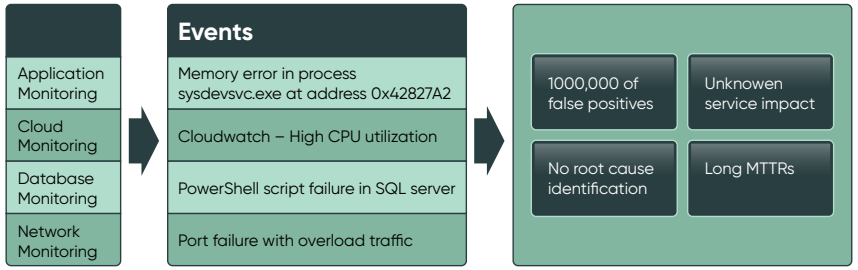
IT delivers mission-critical business services that an enterprise needs to engage customers, increase efficiency, drive innovation, and unlock business insights. These services—supply chain systems, e-commerce portals, collaboration platforms, and others—have to be highly available and responsive. And the long-term impact of frequent service degradations and outages can be colossal—poor business service health destroys an organization's ability to deliver on its promises and drives away customers. Service degradations and outages have an enormous and immediate business impact.

> IT operations continues to drown in a deluge of infrastructure events, without any real understanding of how these events affect business services.

IT operations today is disconnected and lacks visibility

Unfortunately, IT is still plagued by service availability and performance issues. IT operations continues to drown in a deluge of infrastructure events, without any real understanding of how these events affect business services. For example, when a server or network connection fails, IT doesn't know how the failure impacts the business. The failure could be relatively unimportant—or it could be something critical, such as being unable to process credit card transactions. Similarly, when a customer complains about poor response times, it's incredibly difficult to find the root cause since IT doesn't know which infrastructure components support a specific service or how these components are connected.

Multiple disconnected monitoring tools make this situation worse. Each tool generates its own siloed stream of data, and multiple tools often report the same issue. There's a huge amount of noise. A single issue can create thousands of events, and many events are irrelevant secondary symptoms or have no business impact at all. Network operations center (NOC) staff have to manually correlate this information to understand what is actually happening. This is incredibly time-consuming, and errors are common, dramatically increasing the time it takes to fix service outages. Issues are also missed, leading to poor performance and further outages down the road.



> A single service map can take weeks to complete, rendering it obsolete by the time it's complete.

Traditional event management tools aren't service aware

In an attempt to create service visibility, IT software vendors have developed tools that display events on business service maps. These maps show all of the applications, databases, servers, and other IT components that support a business service, with corresponding events attached to each IT component or configuration item (CI).

However, these maps aren't service aware. To provide service visibility, these service maps have to be up to date and accurate—but they aren't. They are typically created using a manual process that requires extensive input from domain experts and application owners. A single service map can take weeks to complete, rendering it obsolete by the time it's complete. And constantly updating hundreds of service maps is a gargantuan task, far beyond the resources of most IT organizations.

Because service maps are inaccurate and out of date, IT operations staff end up misdiagnosing service issues and miss others completely. This makes service outages more severe and prolonged, and it destroys the staff's trust in the very maps that were supposed to make things better. Because of this, these tools fall into disuse, leaving IT back where it started, struggling to deliver the service availability and performance the business demands.

> Machine learning can be used to automatically analyze and process the vast quantity of events being generated by today's IT environments—far more effectively than manually defining and managing event rules.

A different approach to event management

Creating service visibility is only part of the solution. Simply displaying events on a service map doesn't reduce today's overwhelming event volumes. And as business services become more complex and distributed, these volumes are only increasing. IT operations teams are drowning in events, and the situation is getting worse.

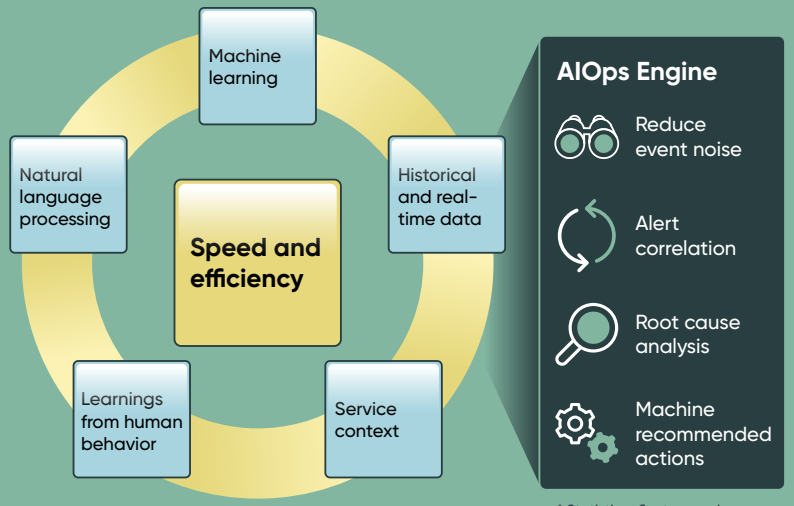
Traditional event management systems use manually defined rules in an attempt to normalize, deduplicate, and filter events, turning them into a smaller number of alerts—but it's not enough. A single underlying issue can generate thousands of events as symptoms propagate over time across the IT environment.

There's just no way to correlate all of these using static rules—there are just too many scenarios to cover. And even if IT could create all of these rules, they would need to be updated every time IT deploys a new application or technology. Even a simple software version upgrade can affect multiple rules, making maintenance a nightmare.

A different approach is needed to keep up with this pace of change. For example, artificial intelligence (AI) can be used to apply algorithms to IT operations (AIOps). Machine learning can be used to automatically analyze and process the vast quantity of events being generated by today's IT environments—far more effectively than manually defining and managing event rules.

Event management systems need to automatically identify topological and temporal event patterns and then use these patterns to correlate event data. By applying this type of machine learning, event management systems can automatically adapt to today's rapidly evolving IT environments, dramatically reducing noise by identifying multiple symptoms of a single underlying issue.

> IT operations staff need a holistic view of everything that impacts service health, not just a list of events.



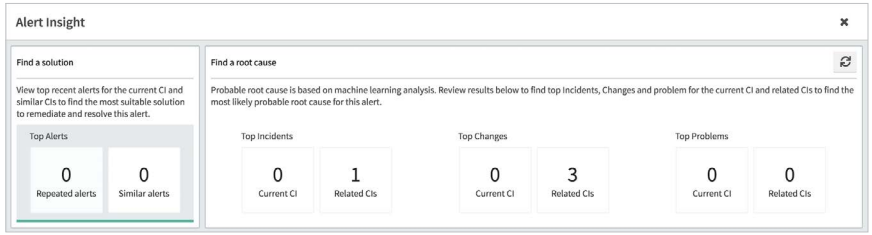
Better experiences using guided flows, intuitive interfaces and one colsole

Isolated events lack operational and business service context

Event management systems incorporating machine learning technologies typically operate in silos. While they have event histories, they don't have access to broader operational data such as incidents and changes. This operational data is critical for rapidly diagnosing and remediating service issues. IT operations staff need a holistic view of everything that impacts service health, not just a list of events.

For example, consider changes. Correlating change and event information is critical since changes are the most common cause of service outages. Unfortunately, IT vendors typically offer separate event and change management tools, making it difficult to see when a change has caused a service issue.

Similarly, by mining historical incident and problem data, IT operations staff can dramatically accelerate diagnosis and remediation of service degradations and outages. By identifying similar issues that happened in the past, they can identify potential root causes for current outages and see what steps were taken previously to fix them. Yet, because events and incidents typically reside in separate systems, there is no easy way to create this bridge, for example, by intelligently pulling up relevant historical incidents in context on event displays.



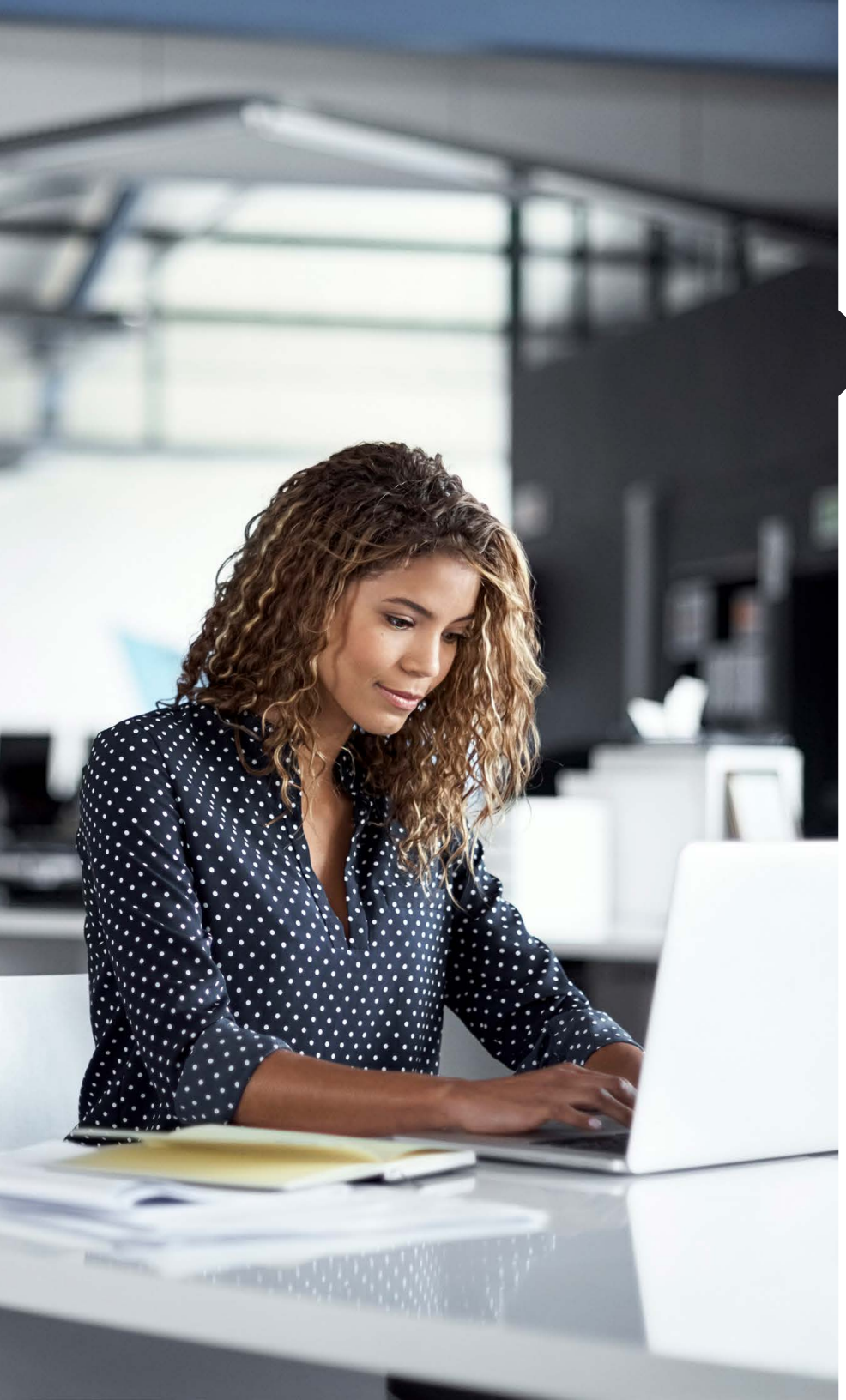
The bottom line

To effectively manage business service availability and performance, IT needs event management to be service aware and intelligent. Displaying a flood of events on an out-of-date business service map doesn't solve the problem. To deliver this intelligence and service visibility, modern event management platforms must:

- Deliver up-to-date, accurate service maps
- Use machine learning to turn a flood of events into clear, actionable service health information
- Accelerate diagnosis and remediation by providing operational context

ServiceNow ITOM delivers intelligent, service-aware event management

ServiceNow® IT Operations Management (ITOM) is a comprehensive IT operations solution that includes Discovery, Service Mapping, Event Management, Operational Intelligence and Orchestration applications. Advanced machine intelligence is used to dramatically reduce event noise, provide service-aware alert correlation, and accelerate diagnosis and remediation of service degradations. ServiceNow ITOM also works seamlessly with ServiceNow® IT Service Management (ITSM), providing instant contextual access to operational data, including incidents, problems, and changes.



Accurate, up-to-date service maps

ServiceNow Service Mapping helps IT operations create accurate service maps in the ServiceNow configuration management database (CMDB) and then automatically keeps these maps and related configuration items (CIs) up to date. A patented service discovery mechanism identifies all of the IT components that support a business service and how they are related. Starting from a service entry point—for example, a URL or message queue—it drills down through applications and IT infrastructure, interrogating each CI in turn to determine its service-specific relationships with other CIs.

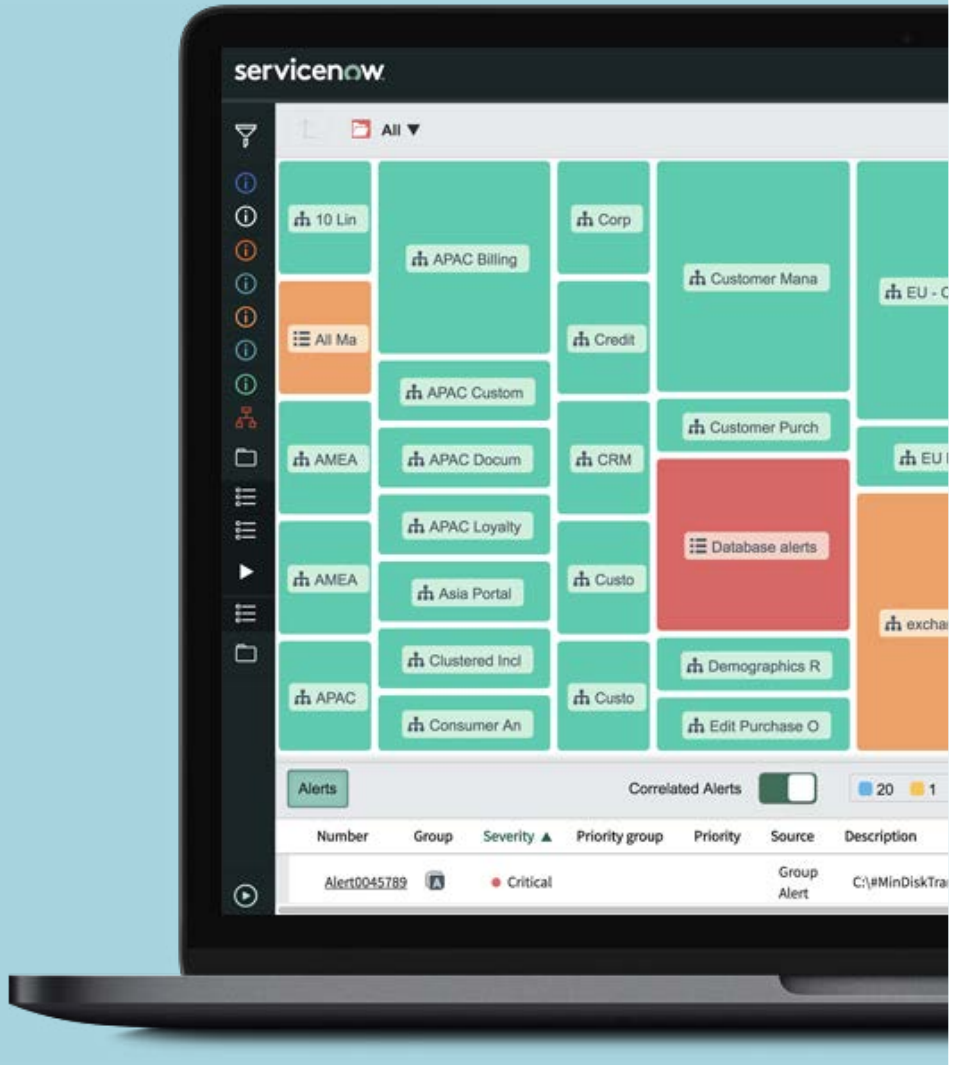
Once Service Mapping has mapped a business service, it keeps the map up to date by automatically tracking service topology changes—including across public and private cloud environments. When Service Mapping automatically detects a change, it updates the service map in the CMDB, maintaining a full change history. Instead of inaccurate, out-of-date business service information, you'll have a complete, current view of how your business services are delivered.

Intelligent, service-aware event correlation

ServiceNow Event Management works seamlessly with virtually all monitoring and event management tools, providing out-of-the-box integrations with leading vendors including Nagios, SolarWinds, Splunk, Microsoft SCOM, HP Operations Manager, IBM Netcool, VMware vRealize, Amazon CloudWatch, and others. It normalizes, deduplicates, and filters events across these sources, significantly reducing event noise by turning them into a smaller number of alerts.

Advanced machine learning techniques are used to correlate these alerts, automatically creating groups of related alerts. This further reduces noise, letting NOC staff see which symptoms are due to a single underlying cause. ServiceNow Event Management does this by learning patterns of repeating alerts and then applying these patterns to new alerts. It provides temporal correlation—sequences of alerts that occur over time—as well as topological correlation, using service maps and other relationships in the ServiceNow CMDB to identify how symptoms propagate across your business services and IT infrastructure.

You can manually add or delete alerts from these automatically generated groups, and you can provide feedback on their usefulness. Event Management learns from this, modifying its future alert grouping behavior accordingly.



As well as grouping alerts, Event Management also assesses their impact on your business services. This goes far beyond simply mapping alerts to specific CIs in the service map. For instance, it weighs alerts to reflect their service-specific impact and adjusts severities to account for redundant service topologies such as service clusters.

Event Management displays this service health information on an intuitive service health dashboard, letting you see the health of all of your business services—or specific groups of services—at a glance. From the dashboard, you can also instantly drill down into individual service maps, which show the health of each component in the map—allowing you to quickly investigate the root cause of service issues.

Rich operational context

ServiceNow Event Management also gives you contextual access to a rich set of operational data, helping you diagnose and remediate service issues faster. Using natural language processing to identify similar alerts that occurred in the past, it gives you a head start on analyzing new alerts. This information is pushed directly to an alert intelligence workspace, letting you benefit from historical operational knowledge.

This historical visibility isn't limited to alerts. Because ServiceNow Event Management runs on the same platform as ServiceNow ITSM, it has full access to incident, problem, and change information. It automatically identifies recent changes that preceded an alert—a frequent cause of service issues. It also automatically retrieves relevant historical incidents, problems, and knowledge articles, limiting the duration and business impact of outages by providing further insights into potential root causes and remediation steps.

Deliver high performance business services with visibility and AIOps

To deliver the service availability and performance your business demands, you need an intelligent, service-aware IT operational management solution. Traditional event management tools aren't up to the task—they aren't service aware, they aren't intelligent, and they lack operational context.

ServiceNow ITOM delivers the intelligence, service visibility, and AIOps you need. With service mapping, it gives you accurate, up-to-date visibility of your business services. Its intelligent event processing dramatically reduces noise, correlating alerts temporally and topologically to help you pinpoint underlying issues—rather than struggling with seemingly unrelated symptoms. And, it intelligently analyzes your operational "big data" such as performance metrics from AWS CloudWatch or Microsoft Azure, giving you real-time insights that help you to diagnose and remediate service outages faster.

Dig deeper into event management at Servicenow.com or talk to your ServiceNow representative today.

Your journey doesn't end here!

Visit our ITOM Health: Event Management page to learn even more about how you can get the most from ServiceNow.

LEARN MORE

ServiceNow was founded on a very simple idea: that work should be easier.
ServiceNow is making the world of work, work better for people. Our cloud-based platform and solutions deliver digital experiences that help people do their best work. For more information, visit: www.servicenow.com.