How to keep your digital services up and running 24/7

The game-changing benefits of AI-Powered Service Operations with Predictive AIOps
Part 1
You’ve got to automate to operate

Digital disruption demands automated solutions

Much of what your IT teams deliver for business transformation is based on digital services and the experiences these services offer your users, both customers and employees. To support your users and prevent operational issues, you rely on feedback from human interactions and from your infrastructure, including your monitoring, performance and logging tools. The data from these two sources ensures services perform as expected and issues are resolved as quickly as possible.

The problem is that your employees are consuming more digital services than ever before, resulting in more service requests. And while service requests are growing, your IT support staff is not. Like employee requests, the amount of data that machines are generating is increasing every day, creating even more activity that your operations teams must manage. Plus, there are these added complexities:

• You have more services transitioning to the cloud that are not part of your traditional, on-premises environment.

• You have new DevOps teams emerging to improve velocity, yet the quality of services and these teams are decentralized from your traditional operations team.

Shannon Kalvar
Research, manager, IT Service Management and Client Virtualization at IDC
Predictive technology and automation to the rescue

With the explosion of digital services, the number of people-generated incidents will double in the coming years as employees demand more from self-service channels and technology. Machine-generated incidents might increase ten-fold as organizations will have more data coming from monitoring, logging, and performance tools.

Together, the sheer volume of incidents generated by people and machines poses a problem that humans alone can scale to address. The answer is automating the management of these incidents and predicting and preventing them before they impact users or the business.

AI-Powered Service Operations predict, prevent, and deflect incidents

Employees and customers alike get frustrated when the technology they rely on to enhance their work lives doesn’t work as expected. What’s even worse is when they finally figure out how to ask for help, they find they must wait for what seems like forever for a resolution. Your overburdened IT teams would love systems that self-heal or, if problems arise, are easy to diagnose and fix. That way, they can spend more time innovating and building the digital business of the future.

You can delight employees with less downtime and faster response times while speeding innovation and agility with AI-Powered Service Operations (AIPSO). This solution will allow you to solve issues brought up by employees, speed change approvals, and predict and prevent machine-generated incidents before they impact users.
AI capabilities and one platform

AIPSO helps your IT teams scale to handle the volume of incidents by staying ahead of issues – predicting and preventing them.

For incidents generated by users (or people), AIPSO automatically deflects work from getting to service teams. Some examples of this are:

- Password can be reset via self-service
- Virtual agents can help employees with common service requests without a human agent ever getting involved
- Intelligent, AI-powered routing can forward issues automatically to the right resolution teams
- Change requests can be automated and accelerated for DevOps

On the machine side, AIPSO automates common operations and predicts outages. Some examples of this are:

- Anomaly detection and alert groupings
- Issue identification and root cause analysis
- Examination of raw logs to predict events
- Pre-built playbooks to resolve issues
- Up to 90% of noise reduction

The key to managing IT issues at scale is automating service operations and having your data, processes and AI capabilities on one platform.
Outcomes of AIPSO

Here are just a few examples of the outcomes you can expect:

**Danske Bank**

Consolidate solutions and centralize all service and operations data and workflows:
Danske Bank accelerated the time it takes to restore services by 6X.

**Magellan Health**

Reduce incident noise from machine data:
Magellan Healthcare managed 75% of incidents via self-serve to reduce dramatically the number of requests reaching the service desk.

**BEACHBODY**

Deflect incidents from employees and customers with virtual agents:
Beachbody reduced the number of outages by 90%.

**Wayfair**

Increase deployment velocity and reduce time spent on manual changes so teams can deliver innovation faster:
Wayfair is able to get service to market faster by leveraging DevOps improvements.
Part 2
Predictive AIOps transforms IT operations

Preventing impact on users
Let’s look at how AIPSO with Predictive AIOps helps your IT teams scale the machine-generated incidents. While AI itself has been around for decades, AIOps is still relatively new – it originated in about 2013. And now Predictive AIOps is yet another breakthrough. At the highest level, Predictive AIOps works with all your existing monitoring tools, and collects data from the source – whether it’s events, logs or metrics, applies machine learning and analytics to identify and help your IT teams fix a problem before it impacts users or your business.

But not all AIOps solutions are equally intelligent. Let’s look at the distinctions between traditional AIOps and Predictive AIOps at ServiceNow.

Traditional AIOps is a good start
In a typical IT operations environment without AIOps, the team is bombarded with thousands of events coming in from siloed monitoring tools across their IT estate – on premises and in the cloud. The team must spend hours to work through all the events when using manual processes and siloed IT tools, and it takes them even longer to determine the impact of an issue on critical business services. But with AIOps, the team can filter out all the noise and look for patterns across large amounts of operational data. AIOps literally turns the thousands of events into the few critical alerts and presents only high priority alerts and impacted services that IT operations should focus on first.

In traditional AIOps, Machine Learning (ML) algorithms are trained to look for only pre-defined patterns on metrics, events and logs. For example, a metric may be monitored for anomalies. Its lower and upper bounds are computed dynamically based on some ML algorithm and an alert is raised if the value of that metric exceeds any of these upper or lower bounds.
Grouping of alerts in traditional AIOps

Another value of traditional AIOps is in the grouping of alerts, which further reduces alert noise and false positives. Several alerts are combined into a single, primary alert so that the IT operations team doesn't have to waste its time analyzing every single alert. For example, we see ML algorithms look for patterns based on the arrival sequence of alerts—time-based correlation. Once the algorithms have learned that pattern, they will group these alerts together if that pattern recurs.

In traditional AIOps, we also see natural language processing (NLP) looking for patterns to cluster alerts based on specific fields, e.g., the alert description, the class of the configuration item and some additional fields. But if you want NLP to group alerts by using yet another field, well, you’re out of luck.

Once a primary alert is identified, AIOps will create an incident that another team will investigate using collaboration tools like Slack or Microsoft Teams. The team may also automatically remediate the issue by creating workflows based on additional insights produced by AIOps, such as related incidents, changes and knowledge articles.

Limitations of traditional AIOps

We have seen Traditional AIOps reduce noise by at least 90%. But while that sounds like a lot, there are two main issues to consider:

• First, that remaining 10% may still be too much for your organization, especially as your systems become more complex.
• Second, these incidents will only reflect types of problems that were expected because ML will run algorithms defined at development time, or later on during operations, to look for a specific fit.

So traditional AIOps:
• Looks for the best fit when applying these pre-defined algorithms.
• Does not adapt to real-life production environments to detect a situation that the operations team had never thought about – therefore, it cannot predict blind spots.

Wouldn’t it be nice if AIOps could learn the “normal” behavior of your infrastructure and applications, then then determine when that “normal” is breached?
What you should expect from a Predictive AIOps solution

Your AIOps solution should be able to predict every possible issue -- known or unknown. Many traditional AIOps solutions require your operations team to know every last possible issue that can go wrong in the environment -- and then configure thresholds for each of these issues. But enterprise and hybrid IT environments are complex and there will always be blind spots. You need an AIOps solution that catches the blind spots and does not have to be told where to look or where to set up thresholds to trigger an alert.

You shouldn’t have to reconfigure an AIOps solution every time there is a change. Traditional AIOps solutions need to be reconfigured when there is a change in the environment -- and this slows everything down. You need an AIOps solution that adapts to changes and resets thresholds on its own.

Your team shouldn’t need special training to use an AIOps solution. Some traditional AIOps solutions require your operations team to learn new skills, new query languages or hire data scientists. And even then, traditional AIOps is still based on queries built by a team that’s expected to know everything that could possibly happen in the environment.

ServiceNow’s Predictive AIOps:

- **does not need** to be told where to look in advance
- **does not need** to be reconfigured when there is a change in the environment
- **does not require** the team to learn a new query language or hire data scientists
The value-add of Predictive AIOps from ServiceNow

Predictive AIOps from ServiceNow gives you an early warning that something is going wrong in your environment that you may or may not even be monitoring. You’ll get an impact description of the potential problem so you can address it proactively.

You don’t have to tell Predictive AIOps where to look. It uses unsupervised learning to determine what is normal behavior based on all the information you tell it to analyze, such as some other fields in the logs. Just tell Predictive AIOps what you want it to examine, and it will add it to its ML models. That’s all you have to do. It adapts to changing environments on its own which means, it constantly analyzes and adjusts normal behavior on its own.

Predictive AIOps is also able to minimize false positives by interpreting the data it sees. For example, it will understand if a sudden spike in the CPU, memory and disk utilization for your shopping cart application is due to an increase in customers ordering online -- which is a good thing. Or, it will determine if there is a rogue process or a memory leak causing an excessive load on the service.

Predictive AIOps can detect issues before traditional AIOps would. For example, running ServiceNow Predictive AIOps in parallel with a customer’s existing, traditional AIOps solution, we detected a VPN connection issue 7½ hours before the traditional AIOps did. Imagine how this can empower your teams to avoid outages. And you don’t even have to be a data scientist, or to set thresholds, rules or complex queries on problems that you think might happen.

Customer examples of predictive AIOps

Let’s look at a couple of outcomes our customers have seen:

One of our customers had to move its brick-and-mortar business online, practically overnight, because of the pandemic. Its traditional AIOps solution did not pick up on a payment application slowing down until it reached the established threshold. Since ServiceNow Predictive AIOps was running in parallel, it picked up an anomaly 78% faster than the traditional AIOps solution, reducing the resolution time by 40%. This resulted in the customer retaining more than a thousand orders worth about $270K.

ServiceNow itself avoided a massive VPN outage when ServiceNow Predictive AIOps detected an LDAP server had slowed down. The outage could have impacted about 3,600 users when they would have come online. But ServiceNow was able to resolve the issue as soon as it happened – and before employees were affected, preventing 1,800 hours of lost productivity and saving about $117,000.
Part 3
How it works—deep dive into ServiceNow
AIPSO with predictive AIOps

Single system of record

AIOps combines big data and machine learning (ML) to automate IT operations processes, including event correlation, anomaly detection and causality determination. Our approach is to bring in the monitoring event data from monitoring sources, then correlate events and identify root causes with our AI/ML capabilities. Additionally, we identify anomalies from log data to predict service issues.

Platform and integration services are the set of capabilities associated with the operationalization, integration and use of the AIOps, monitoring and logging features. Our IntegrationHub capability, which is at the core of the ServiceNow platform, connects to other platforms and tools across the enterprise to provide our customers with a single system of record.

Figure 1: ServiceNow Predictive AIOps workflow enables 99%+ noise suppression
**Platform for AIOPS, SRE, DevOps and SecOps**

Having a single system of record is critically important. In an ideal AIOps world, there would be a data lake of data from all monitoring systems. In reality, data is stored separately by each monitoring tool in its own database. ServiceNow provides a holistic approach to AIOPs by combining key capabilities from ITSM, ITOM, DevOps, SecOps and Integration Hub, delivered on the Now Platform. Shown in figure below, AIOps data, processes, and automations are seamlessly shared on a single platform.

*Figure 2: Data stored in silos creates chaos. The Now platform brings data together.*
To drive more value from AIOps, ServiceNow customers are integrating service and operations powered by AI and ML. For example, when the service desk gets too many incidents from operations, AIOps can predict and prevent issues before they ever become incidents or outages and also reduce event noise. It reduces the sheer number of incidents from inundating the service desk, resulting in lower operational costs as well as an improved experience for both agents and customers.

**Figure 3: AI-Powered Service Operations delivers more value on the ServiceNow platform**

To enable operations automations, the Now Platform takes events, logs and metrics from sources in real time and acts as an intelligent automation engine to predict, prevent issues and automate resolutions.
Predictive Intelligence (PI) for faster resolutions

We call this capability Predictive Intelligence. In ITSM, it helps reduce the time to repair and saves service agent productivity by automating the actual assignment of an issue to the right resolution group. Employees simply submit a simple description of the issue they are having and Predictive Intelligence taps months of history and potentially thousands of previous incidents to accurately categorize the incident, prioritize it, and assign it to the right team—helping to eliminate human error and speed time to incident resolution.
Visibility and a top-down approach to ML-based Service Mapping

Having visibility helps you to be proactive verses reactive. AIOps first obtains visibility into the services and infrastructure that IT is managing. Step one is gaining actionable insights from gathered data from varying sources. ServiceNow Discovery, scans networks and public and private clouds to find IT infrastructure and applications and stores that configuration information in the ServiceNow CMDB. ServiceNow ML-based Service Mapping uses a top-down approach to create topology maps that relate services to supporting IT infrastructure, analyzing actual infrastructure configurations and storing the maps in the CMDB.
Intelligent traffic-based mapping for getting visibility rapidly

One service mapping option that allows you to discover and chart services in minutes is intelligent traffic-based mapping, which leverages traffic connection information in your CMDB to identify service-level relationships between previously discovered CIs. This traffic data is collected by ServiceNow Discovery, and you can also import VPC and NetFlow logs. In the past, traffic-based mapping approaches cast a fine net, identifying every connection between CIs rather than focusing on important service-level relationships. This resulted in a highly inclusive service map, but it also meant the map had many irrelevant components and relationships that had no significant impact on the application service. This clutter made the map difficult to use because it was hard to identify key infrastructure and relationships.

Intelligent traffic-based mapping addresses this issue by using machine learning to identify significant relationships. It scores each relationship, giving you a ranked list where you can choose which relationships you want to include in the service map. This results in a much more focused map, although it is not as precise as top-down mapping. It does, however, require much less effort than top-down mapping, making it a good option for bulk mapping of less critical services. And because it uses traffic data, you can also use it to extend top-down maps to include CIs for which there is currently no mapping pattern.

Figure 6: Intelligent traffic-based mapping
Intelligent traffic-based mapping is also a good option for mapping applications that have not been fully discovered. It works seamlessly with application fingerprinting, a ServiceNow Discovery capability that uses machine learning to identify applications. Application fingerprinting categorizes and classifies running processes collected during basic discovery, creating groups of processes that represent potential applications, including custom applications and new off-the-shelf applications not yet supported by ServiceNow Discovery. By creating CIs for these fingerprinted applications and then using intelligent traffic-based mapping to identify service-level relationships, you can quickly build service maps without having to create patterns to fully discover the application.

**Alert correlation to identify root causes**

With service mapping completed, ServiceNow AIOps can collect events from monitoring tools, processes them to create alerts, and applies ML to automatically group—or correlate—them. You can treat grouped alerts as a single phenomenon to take actions on a group, such as opening an incident. When you use alert groups with service maps, you can also leverage them to identify a root cause alert.

![Figure 7: ServiceNow provides a visibility of service health across organization](image)
Anomaly detection with metrics
Another tool for understanding root causes of incidents is ServiceNow Metric Intelligence that detects system behavior that falls outside normal parameters. Analyzing performance data coming from any environment, ML algorithms model metric behavior to automatically identify operational thresholds, adjusting for seasonality where relevant. This removes the burden of manually adjusting thresholds for hundreds or thousands of metrics.

Anomaly detection with logs
Predictive AIOps and specifically Health Log Analytics (HLA) also uses ML to process logs and create a baseline of normal operational patterns. Once an anomaly is detected, HLA creates an alert with a prediction that an anomaly may cause an issue.
Most customers should focus on integrations and automation for the problem identification and resolution process; integrations with ITSM, monitoring and observability (APM) solutions, and runbook solutions (while utilizing AI/ML models); anomalies correlated with historical analysis; and the use of automated actions and process workflows that match the right data with the best-fit people. The holistic approach of tool rationalization with the alignment of people, process, and technology is a critical success factor for modern digital operations. The need to consider these factors, along with automation and analytics, provides a foundation for enabling more streamlined business value delivery capabilities. The results often drive improvements in customer satisfaction (i.e., NPS metrics), decreases in the time needed to resolve problems, reduced service desk calls and tickets, and increased teamwork and collaboration.

*Stephen Elliot*
Program Vice President, Management Software and DevOps, IDC

**Automation with Flow Designer**

Automation is at the heart of Predictive AIOps and all of the capabilities we’ve discussed above. ServiceNow’s workflow engine drives the automated actions across ITOM, ITSM, DevOps, and SecOps. The automation engine (called the Flow Designer) is available to all ServiceNow applications. You can use it to automate business processes (workflows), such as restarting servers, updating CMDB, closing incident, provisioning cloud services, and so on.

![Flow Designer](image)

*Figure 10: Flow Designer drives the AIOps automation workflows*
Conclusion: what ServiceNow AI-Powered Service Operations and Predictive AIOps mean to your business

For service management
- 30% fewer service desk requests that require human intervention
- 12% service desk agent time savings thanks to automatic request routing based on machine learning and predictive intelligence
- 16% of common issues deflected and automatically resolved

For operations management
- 99% event noise reduction enabling you to manage events easier, proactively and cost-efficiently
- $1 million per year in savings on average
- 25 - 35% fewer priority 1 outages, (i.e., major incidents)
- 40% reduction in mean time to resolution

Once you gain confidence in the results you see with AI-Powered Service Operations and Predictive AIOps, you will reach the nirvana of self-healing operations to better meet the needs of IT, the business, customers and employees.

Learn More