

How AIOps platforms help agencies

‘KNOW THE TRUE HEALTH OF THEIR IT SERVICES’

FedScoop Report

System outages across the U.S. during the pandemic highlighted the need for agencies to attain system-wide visibility and automation tools.

The IT specialists who keep the nation’s government IT systems running are used to operating unseen behind the scenes. Often underappreciated and underfunded, they nevertheless serve the public in countless ways by tending to the digital engine rooms that drive and deliver government services at a scale few can appreciate.

That is until those services fail — as many did last year when virtually all 50 states saw their websites and backend IT systems crash as millions of Americans suddenly sought unemployment relief and other aid in the wake of the pandemic.

States weren’t alone. Federal agencies were similarly overwhelmed trying to process and issue emergency business loans. Not since the ill-fated launch of HealthCare.gov in 2013 has government experienced the kind of crush in demand and collapse in service that citizens encountered last spring.

Many of those same agency IT specialists were fortunate in being able to turn to a variety of cloud-based solutions.

If there was one upside to the turmoil, though, it may have been the sudden string of decisions by governors to green-light remedies that IT departments had long been requesting, observed Wylie Vasquez, leadership advisor for observability and AIOps markets at Splunk. Facing enormous pressure to pinpoint what was triggering government unemployment benefits sites to crash, it wasn’t long before agencies began calling Splunk for help, according to Vasquez.

Fortunately, Splunk was able to respond quickly, using Splunk’s *IT Service Intelligence (ITSI)* analytics and IT management solution. ITSI is a part of a new generation of so-called *AIOps platforms* that give IT administrators the ability to collect, unify and analyze data from a vast range of products and applications in real time — and then respond to known and previously unknown anomalies automatically.

Aligning IT with citizen expectations

Those widespread system outages illustrated not only the need for more powerful tools, like ITSI, but also “the importance of aligning IT systems and operations more directly with the need to deliver digital citizen services at a level the public expects,” Vasquez said.

That alignment takes on even greater urgency and importance for agencies where a lot of money is coming in and going out, where there’s a greater risk of fraud and where 24/7 availability and performance are crucial, he added.

Government agencies have come a long way in delivering services digitally. One example is the growth in tax returns filed electronically, from 57% of returns submitted in 2007 to more than 90% recently, according to figures cited in a *report on government customer service* from consultants at Deloitte.

However, from the view of the American public, citizen satisfaction with government customer services varies widely *among federal agencies*; and in aggregate, it is at its *lowest level since 2007*, according to the American Customer Satisfaction Index (ACSI). And that was before the pandemic.

“



Everything is changing all the time. So the stand-in is to use visibility across all of your infrastructure so that you don’t have blind spots.

– Wiley Vasquez, Splunk

Citizen satisfaction is ultimately judged as a measure of perceived performance minus expectations, according to William D. Eggers, executive director of Deloitte’s Center for Government Insights and Bruce Chew, managing director with Deloitte Consulting in the report. While agencies have limited control over consumer expectations, they can take greater control in understanding how citizens interact with agency data systems — and in acquiring the right tools to improve performance.

Taming complexity with visibility

Aligning government IT systems to fulfill the needs and expectations of citizens, however, remains easier said than done, even for the best-managed IT departments. That’s due in part to the administrative layers routinely separating IT staffs from the citizens that agencies endeavor to serve, and in part to the sprawling complexity of most agency IT systems.

As Vasquez put it: “You take years and years of all of this technical debt — new technology layered on top of old technology — and the rapid changes going on in the organization; and add in different SLAs [service level agreements] that are not even tied to the end users, and you get a big ball of complexity. Everything is changing all the time. So the stand-in is to use visibility across all of your infrastructure so that you don’t have blind spots,” he said.

What IT teams ultimately face is “a really, really hard big data problem to solve. ITSI allows enterprises to bring all that data together and pre-analyze it, so they can avoid a lot of those ‘War Room’ calls,” he said.

The Census Bureau’s digital overhaul

ITSI gives agencies more than a window into their legacy operations; it also provides a powerful tool for managing large-scale development projects.

That was the ***case at the U.S. Census Bureau***. When Census officials made the bold decision to conduct the 2020 decennial census online, instead of relying on mailed surveys, it was clear from the start that the bureau would require a whole new approach to their IT, security and data operations.

That meant not just assembling the right technology to collect and process census data on 330 million people. It also meant having tools that could operate on a large scale to reduce all kinds of technical risks, not to mention political concerns. And all of it had to be deployed in a compressed time frame when most experts agreed, the 2020 census was already underfunded.

A critical step in addressing those challenges, according to Vasquez, involved bringing all of the bureau’s existing mission-critical applications and platforms, including Oracle OEM and AppDynamics, into Splunk’s ITSI AIOps platform, creating a single pane of glass view of the bureau’s applications.

Prior to that, pinpointing the root cause of an issue meant separately searching through all of the tools tied to the IT operations. With ITSI and its event analytics dashboard, bureau IT administrators could now readily identify or narrow the source of an issue across their technology stack, using an automated AI and machine learning approach.

Another advantage of ITSI, according to Vasquez, is the AI/ML and predictive analytics capabilities it provides the Census Bureau and customers more broadly, to predict and prevent common issues of the past, before they happen, reducing wasteful costs in time and resources.

While no one could have fully foreseen the impact of the pandemic on the 2020 Census, most experts agree the Census Bureau’s online platform performed better than many expected, and actually helped the bureau navigate through the pandemic.

Moving into the AIOps era

As agencies and large scale enterprises continue to rely on distributed IT services, the need continues to grow for high-performance AIOps platforms like Splunk *ITSI*, and other tools like *Splunk Infrastructure Monitoring* and *Splunk APM* — recognized by Gartner as a “visionary” application performance monitoring platform.

AIOps platforms have become an essential tool for contextualizing large volumes of varied and ever-changing data. What distinguishes AIOps platforms from more traditional analytics tools is their ability to automate routine practices and increase the speed and accuracy of issue recognition. That enables IT staffs to focus more of their attention on higher value needs.

There are five primary use cases for AIOps platforms, according to *analysts at Gartner*:

- 1

Performance analysis: The volume, variety and velocity of data has exploded beyond anything humans can handle. AIOps applies sophisticated techniques to analyze bigger data sets, to identify and prevent performance problems before they happen.
- 2


Anomaly detection: Machine learning is especially efficient at anomaly detection, by identifying data events and activities that stand out from historical data — including anomalies they haven’t been seen before and without explicit algorithms to signal an alert.
- 3

IT service management: AIOps lets IT professionals manage their services as a whole rather than as individual components. They can then define system thresholds and automate responses to align with their ITSM framework, helping IT departments run more efficiently.
- 4

Event correlation and analysis: Traditional IT tools are better at sounding alarms than providing insights into underlying issues. AIOps can automatically group notable events based on their similarity. That reduces unnecessary noise and the burden on IT teams to sift through conflicting signals.
- 5

Automation: Legacy tools require cobbling information together manually from multiple sources before it’s possible to understand, troubleshoot and resolve incidents. AIOps dramatically accelerates that work, by automatically collecting, correlating and analyzing multiple data sources and taking steps to respond to abnormal conditions.

In choosing a AIOps platform, Gartner’s analysts said it’s important to understand that a true AIOps platform isn’t just a collection of tools. Rather a fully-functioning AIOps platform must be capable of gathering all the necessary data at full fidelity, not just aggregations or rollups. They must be able to enrich, analyze and crunch that data and deliver meaningful conclusions and insights, without requiring heavy amounts of custom configuration and maintenance work. And they should be able to automate the right responses at the right time across an enterprise’s ecosystem.



ITSI allows enterprises to bring all that data together and pre-analyze it, so they can avoid a lot of those ‘War Room’ calls.

- Wiley Vasquez, Splunk

One reason agencies continue to turn to Splunk’s Data-to-Everything platform, according to Vasquez, is it’s unique strengths in being able to ingest and unify nearly any kind of data — structured or unstructured, including logs, metrics, text, wire, API or social-media — from nearly any tool and any system, on-premises or in the cloud. Once assembled and unified, it then becomes far easier to apply AI and ML to get ahead of problems before they happen.

But Vasquez also stressed that the power of a tool like ITSI still depends on whether agencies are viewing the performance of their systems from the lens of their customers.

“The number one thing organizations should ask themselves up front,” concluded Vasquez, is, “Do they know the true health of their services?”

That includes asking, “How much at risk are they from a security standpoint? Do they have all these failed points — from all the complexity — monitored in a way that they can react to quickly, if something does go down? Do they have the right kind of predictive analytics, so that things don’t go down? And then, do they have a visibility from the customer’s experience?”

Learn more about how Splunk’s Data to Everything Platform can help your agency improve performance and citizen’s user experience.

This article was produced by FedScoop and underwritten by Splunk.

Benefits of using Splunk AIOps

45%

reduction in high-priority incidents & outages

35-45 min.

advanced lead time to predict imminent outages

90%

reduction in incident investigation time

95%

reduction in event noise

Source: Splunk