gaining end-to-end visibility: better IT operations through operational intelligence

splunk>

industry perspective

executive summary

The speed of innovation in government today is astonishing compared with where the public sector was even just a few years ago. In order to meet needs and rising citizen demands, government IT has turned to the cloud, virtualization and complex data centers.

But while efforts to meet the demands of today's environment are admirable, they've also introduced significant challenges into the IT operations of the public sector. How do you monitor these environments? How do you automate systems? How do you ensure everyone is on the same page and moving in the same direction when shifts in technology or deployments of code are moving quickly? How do you gain visibility into all of your assets? And when something breaks, or if there's downtime on an application, how do you know when and where it happened, and how do you fix it quickly?

Turning to Operational Intelligence can reduce the obstacles that those in public sector IT operations face. Operational Intelligence is the analysis of machine-generated data to provide new levels of visibility, information and insight. Using analytics and intelligence drawn from the logs of machine data, you can gain this operational visibility into the layers of your environment and turn the silos of machine data generated in your data center into integrated and actionable information.

This helps you reduce your mean-time-to-investigate (MTTI) and mean-time-to-recovery (MTTR), keep your critical services running and to find and fix problems faster than ever before. This also means that IT staff is freed up to do more sophisticated, innovative, mission-critical work.

To further understand how Operational Intelligence can improve your agency's IT operations, GovLoop partnered with Splunk, the leading platform for Operational Intelligence that enables you to look at machine data and find important insights. Bill Babilon, IT Operations Specialist for Splunk Public Sector, reveals the current challenges to public-sector IT operations; why it's so critical that they be addressed and how operational intelligence can give you better end-to-end visibility across all of your platforms so you can deliver essential services and applications to meet mission need and citizen demands.

the current state of IT operations in the public sector

To understand why IT operations is so critical to the effectiveness of today's public sector, you must first understand what IT operations is.

Put simply, IT operations is the process of managing and monitoring the day-to-day IT infrastructure of an agency and troubleshooting any issues as they arise. This includes managing the provisioning, capacity, performance and availability of the computing, networking and application environments. Good IT operations is absolutely necessary for government, as they continue to be responsible for more efficiently delivering better services and applications both internally and externally.

But there's more to IT operations than just keeping things running.

"There are really two dimensions to IT operations for the public sector," Babilon said. "One is the essential part, which is keeping the lights on in the data center. It's also running and monitoring the basic physical infrastructure, and also the applications on top of that infrastructure that your agency depends upon."

The second layer, Babilon explained, is being able to maintain a proactive IT operations approach, one where you're able to detect problems as they arise or even predict them before they happen.

"Today more than ever, public sector IT needs to be able to predict where they're going either from a capacity point of view or an operational expense investment," he said. "You don't want to just wait until you have an operations issue, then race off to fix it."

How can you be proactive and predict issues before they happen?

That's where the public sector IT operations landscape faces its biggest challenges. Today's data center has evolved. It's now a complex, layered group of siloed and interconnected technologies working in an environment without boundaries. When problems arise, finding the root cause or gaining visibility across the infrastructure to identify and prevent outages is nearly impossible. Meanwhile, virtualization and cloud infrastructures introduce additional complexity and create an environment that is more difficult to control and manage.

Additionally, reduced budget and legacy IT systems create another obstacle for agencies looking to improve their IT operations. Traditional tools for managing and monitoring IT infrastructure are out of step with the constant change happening in today's data centers. These systems are inflexible, cost too much and are not architected for the complexity of today's environments. Designed for a single function in IT, they do not work across multiple technologies to help solve problems. Further, their monitoring approaches are often based on filtering and summarizing. When problems arise, they typically lack the ability to drill down and provide granular analysis of IT data. Linking the various causes of performance issues and outages is especially challenging because traditional tools are siloed and can't access and analyze all the relevant events across the IT landscape.

As the public sector moves more and more to virtualization and cloud computing, it's critical to gain visibility across all components of their dynamic and complex environments to correlate problems occurring in one layer of the stack with key performance indicators in another. For example, an agency may detect that one application's performance may be slower, not because of something in the application, but because its virtual machine got moved to a different host with less memory. How can they know that?

The answer lies in better Operational Intelligence.

better IT operations through machine data & operational intelligence

Machine-generated data is one of the fastest-growing and most complex areas of big data.

It's also one of the most valuable, containing a definitive record of all user transactions, customer behavior, machine behavior, security threats, fraudulent activity and more. It contains a definitive record of all the activity and behaviors of customers, users, transactions, applications, servers, networks and mobile devices. And it's more than just logs. It includes configurations, data from application programming interfaces, message queues, change events, the output of diagnostic commands, call detail records and sensor data from industrial systems and more.

This machine-generated data holds critical information on user behavior, security risks, capacity consumption, service levels, fraudulent activity, customer experience and much more.

Operational Intelligence means turning these massive amounts of machine data into valuable insights, giving you a real-time understanding of what's happening across your IT systems and technology infrastructure so you can make informed decisions.

Splunk's IT operations solutions enable you to examine your data in depth and in real time from across your IT environment — whether on premise, in the cloud or hybrid. Splunk's software collects and correlates the machine data needed, so you can quickly troubleshoot issues and outages, monitor end-to-end service levels and detect anomalies. This allows you to reduce MTTR, lower monitoring costs, improve system uptime and support strategic initiatives like data center optimization and tool consolidation.

"What Splunk allows you to do is pull data from each of your IT layers and mix it all together in a time synchronized manner," Babilon said. "Splunk brings in raw data, we time synchronize it, and we put it in a common place. Then you can do a simple keyword search for errors so that you're able to see the beginning of a failure and start tracking it through different levels of the system." This ability also means that, for the user, when data is collected once, it can be used many times across the Splunk platform.

benefits of splunk for IT operations:

Reduce mean-time-to-resolution with rapid, data-driven troubleshooting

Proactively monitor infrastructure by correlating events across a variety of machine data

Transform IT service monitoring with analytics delivered by Splunk IT Service Intelligence

Eliminate silos by integrating data from across your infrastructure and systems

Detect anomalies and prevent problems in real time

IT operations bolstered by Operational Intelligence to more quickly detect and troubleshoot issues benefits your agency in multiple ways:

radically cut downtime:

Splunk, for most organizations, acts as a way to quickly find a needle in a haystack – or in the case of large scale, virtualized environments, multiple needles in multiple haystacks. With Splunk, you can radically cut downtime and outages – in fact, Splunk customers typically experience a 70-90 percent reduction in MTTR. Its powerful search language helps you connect the dots across the heterogeneous systems in your environment. This gives you the ability to perform rapid ad hoc searches, or routine investigations across your entire infrastructure from one place, so you can dramatically reduce the time it takes to resolve issues.

proactively monitor end-to-end:

Because Splunk retains all the data from every single element of your infrastructure without filtering, you can use it to proactively monitor for problems before they impact users and services. Splunk provides complete visibility across the full application context, so your agency can better prioritize where to take action.

deliver real-time operational visibility:

Splunk retains knowledge from past outages, and monitors real-time data so you can correlate events, changes in metrics across every tier of your infrastructure and gain deep insights into anomalies or deviations from steady states. Now, instead of managing and maintaining multiple tools, you'll only need one – one that has authenticated role-based dashboards and views for your different stakeholders.

Finally, when your agency's IT department doesn't have to spend the bulk of its time and budget on maintenance, troubleshooting, and "keeping the lights on" for IT, it can work on more mission-critical projects and innovate better.

"The majority of the average IT organization's yearly budget is spent on maintenance type issues, keeping the lights on, and not creating that new value, or not meeting that next need or fulfilling that next request of the citizen. But with what we offer, we're able to reduce that time to resolve the amount of effort that's spent on maintenance that now frees up budget and personnel, so you can begin to be innovative and work on that next important mission-centric idea."

-Bill Babilon, IT Operations Specialist, Splunk Public Sector

PHOTO: MESA0789 BY CC 2.0

case study: seeing patterns in statistics to better support public safety

The police department for the city of Chandler, Ariz., just outside Phoenix, has its own technology staff to improve delivery of police related services and increase security for confidential records, data and processes.

In particular, it maintains a network that links the main police station and two satellite facilities. With 320 police officers and thousands of activities, incidents and investigations happening each year, the department needed a better way to track the performance of mission-critical applications such as a computer-aided dispatching system (CAD) that stores calls from citizens and a records management system (RMS) that is the repository for all activities across the department.

The department needed to monitor the data from multiple web servers and systems in order to improve delivery of police related services, but it lacked full operational visibility into its virtualized environment. To solve this issue, it turned to Splunk.

By indexing logs from these applications and visualizing the data in dashboards, Splunk Enterprise has enabled the department to track the health of its infrastructure, ensure the availability of its systems and proactively address potential problems.

The Chandler Police Department also uses the Splunk App for VMware to monitor machines and servers in the department's virtualized environment, allowing staff to maximize utilization and anticipate when a system will be overtaxed.

Finally, using the Splunk DB Connect application, which allows the indexing of structured data, the Chandler Police Department has eliminated the costs of programming and is able to enrich data gleaned from machine generated logs with statistics from the records management system (RMS) database, allowing for deeper analytics and greater insights.

"I never thought that Splunk could be such a useful law enforcement tool," said the police department sysadmin. "Splunk Enterprise lets us query our data like a Google search. We connect the dots and see patterns once hidden in all the statistics. We're improving services, operating smarter and giving the public greater returns on its tax dollars."

conclusion

The ongoing fragmentation of IT across different services, providers and technology creates restrictive data silos and a lack of visibility across agencies.

Across all levels of government, the need for a central, unified view into IT operations is growing. When fulfilled, this holistic view enables IT departments to have more time for user centric, mission-critical work rather than frantic troubleshooting.

Government has the data, and the answers are out there to government's most pressing questions.

"But the answers are locked up in silos that governments just don't have the visibility to see," said Babilon. "That's the value of Splunk. The company can help you look for the thread and guide you from the reactive fix to the proactive solution. The folks who really get the value out of Splunk's platform are the ones who not only keep the lights on in their IT operations, but are also looking at what's happening down the road."

By gaining end-to-end visibility into all operations through Splunk's platform and Operational Intelligence, agencies will be able to identify problems in real time instead of spending valuable time combing through massive amounts of log data from each system. In turn, real-time visibility and contextual insights enable organizations to look into the future and better predict what's going to happen next.

---

about splunk

Splunk Inc. provides the leading platform for Operational Intelligence. Splunk® software searches, monitors, analyzes and visualizes machine-generated big data from websites, applications, servers, networks, sensors and mobile devices. More than 11,000 organizations use Splunk software to deepen business and customer understanding, mitigate cybersecurity risk, improve service performance and reduce costs.

splunk>®

about govloop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

www.govloop.com | @GovLoop

govloop

1152 15th St. NW, Suite 800
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com
@GovLoop