DeKalb County School District Supports Academic Excellence With Splunk Platform

DeKalb County
School District

Executive summary

Georgia's DeKalb County School District is a national leader in science, technology, engineering and math (STEM)-certified schools. As part of the district's mission to inspire educational excellence, it has committed to providing an equitable and accessible 21st century learning environment supported by the use of emerging technologies. To further its educational initiatives, the district needed better visibility into its IT infrastructure. Since deploying Splunk Enterprise and Splunk IT Service Intelligence (ITSI), the district has seen benefits including:

- Preventing network outages and providing secure and reliable IT services
- Reducing mean-time-to-investigate and repair IT issues
- Supporting the district's mission of educational excellence

Why Splunk

In the past, DeKalb County School District's six IT divisions operated in silos; staff who managed critical systems that made up the IT network relied on various tools installed on their personal computers, leaving management all but blind to what was happening. When an issue occurred, from problems accessing the network or student resources to a fiber cut or losing access to an HR department application, customers often created incident tickets through the help desk system or an email.

Typical issue resolution involved sending a technical expert or engineer to the site to assess the issue. With a lack of visibility into incident contributing factors, it could take up to several days to investigate and repair IT issues. This affected the district's students, teachers, employees, parents and community stakeholders who expect seamless access to resources. The district needed better IT visibility to improve its network security and infrastructure operations.

"At a Gartner event, Splunk software surfaced as a leader in the SIEM Magic Quadrant and we decided to bring it in to solve our operational issues," says Gary Brantley, CIO, DeKalb County School District. "We were amazed by its ability to not only identify, but anticipate issues and prevent them from happening in the future. That was one of the key reasons why we went with the Splunk platform."

Industry
- Public Sector
- Education
- Nonprofit

Splunk Use Cases
- IT operations
- Security

Challenges
- Needed to support educational mission to inspire educational excellence
- Management lacked visibility into divisions within the IT department
- Network outages and other issues affected students and district personnel
- Wanted to reduce time-consuming issue investigation and resolution

Business Impact
- Supports educational excellence and commitment to providing an equitable and accessible 21st century learning environment
- Proactive monitoring prevents network outages and reduces impact on stakeholders
- Provides reliable and secure IT service to students, teachers, staff and community stakeholders
- Reduced mean-time-to-investigate and repair IT issues from days to minutes

Data Sources
- Microsoft Windows, Active Directory, Office 365
- Student information systems
- Routers
- Switches
- Firewall
- Servers
- Linux

Splunk Products
- Splunk Enterprise
- Splunk ITSI

Proactive monitoring of district "IT engines"

With Splunk Enterprise and Splunk ITSI in place, the district has gained visibility into IT operations that it lacked previously. Now, the first staff to arrive in the morning can quickly see how the district's "IT engines" are running and performing. The district's CIO and manager of enterprise systems now depend on Splunk ITSI, which combines machine data with machine learning for an analytics-driven approach to IT operations.

One example of how Splunk ITSI has added value is improved application performance during critical student testing. IT staff monitor the online testing application, while also monitoring other applications that are being used simultaneously and could impede the testing application's performance. With powerful visualizations in Splunk ITSI, staff can shut down other applications or switch up resources to make sure the core application in use at that time is running at high optimization. The CIO notes that without Splunk ITSI, this effort would have been like looking for a needle in a haystack, but with these pre-built solutions his team has intelligent visual clues that enable the applications to run smoother.

"Splunk ITSI is a necessity. Without Splunk ITSI, I would not have a clear understanding of our end-to-end operations," Brantley says. "I recommend Splunk ITSI to other school districts, to automate monitoring and gain immediate insights with powerful visualizations, because it absolutely will allow every organization to run a lot more efficiently."

> "Splunk ITSI is a necessity. Without Splunk ITSI, I would not have a clear understanding of our end-to-end operations. I recommend Splunk ITSI to other school districts, to automate monitoring and gain immediate insights with powerful visualizations, because it absolutely will allow every organization to run a lot more efficiently."

Gary Brantley
CIO, DeKalb County Schools

Unified view of critical IT services

By combining Splunk Enterprise and Splunk ITSI with a Network Operations Center (NOC) staffed with cross-departmental personnel, the district now has better visibility into network security and enhanced communication about IT system status.

"For us, the biggest challenge in the past, by far, was visibility into our network," Brantley says. "We found ourselves constantly guessing at the root cause of issues. With Splunk ITSI, we have a single place to visualize what is happening in an easy color-coded way to understand how the network services are running at any given moment."

DeKalb has gained Operational Intelligence through Splunk Enterprise and Splunk ITSI. Along with the district's newly developed in-house communication system, D.I.R.T. (DeKalb Incident Response Team) for IT troubleshooting, the district has quick and streamlined communication to all parties that need to be in the loop. These new capabilities also enable district personnel to communicate faster with the schools to keep them informed of the repair status.

Download Splunk for free or get started with the free cloud trial. Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.

splunk>

✉ sales@splunk.com   🌐 www.splunk.com