splunk> turn data into doing™

CASE STUDY

Jeffco Public Schools Enables Secure 21st-Century Learning with Splunk Enterprise

Key Challenges

Modernizing learning meant making computer resources available to students anytime, anywhere — which demanded increased uptime and exposed the school district to new security vulnerabilities.

Key Results

Jefferson County Public Schools now delivers a safe, innovative learning environment with improved security, increased reliability and better protection against cyberbullying.

JEFFCO PUBLIC SCHOOLS

Industry: Education

Solutions: IT, Security, Platform

Learning in the 21st century presents an array of unique challenges and opportunities.

Colorado's Jefferson County Public Schools (Jeffco) is a K–12 district devoted to preparing great 21st-century learners — a mission that requires technology to ensure a high-performing, flexible and secure learning and teaching environment.

Securing the Student Experience

When Jefferson County Public Schools set up a wireless network to make computer resources available to students, it also opened itself up to account credential theft and unauthorized access. In response to this vulnerability, the district turned to Splunk to provide robust security and to maintain open networks for flexible access to information.

"We have 100,000 users on our network — 250,000 users if you count family members. Account credential theft was one of the biggest issues that we wanted to resolve by implementing Splunk®. We needed to correlate user activity consistently across all of our devices and systems," says Chris Paschke, Jeffco's director of data privacy and security. "And while we're also protecting sensitive data, we need to provide reliable access to support teaching and learning innovation."

Data Driven Outcomes

86k
students and 15k employees across 156 sites benefit from reliable IT services

99.99%
wireless uptime enables students to learn without IT interruptions

100k
devices across 700 square miles now with improved security

District Size, Complexity Pose IT Challenges

One of the biggest challenges for the Jeffco team is ensuring a secure experience across the district's large and complex network. Paschke's five-member security team supports 86,000 students and a staff of 15,000 in 156 geographically distributed schools with firewalls, email gateways, investigations and other security defenses. In addition to providing connectivity for 95,000 district-owned devices such as Chromebooks, the team also has to maintain wireless network security for up to 100,000 connected users.

"BYOD poses particular security risks because devices can come in harboring viruses, and it can be difficult to monitor their use," Paschke says.

Prior to deploying Splunk, investigators had to look through numerous system logs to detect the source of malware or a phishing attack. The lack of holistic visibility hampered incident investigations and forced IT staff to wait hours for the results of individual queries.

In addition, IT staff also had to closely monitor physical security cameras that were saved to hard drives and subject to heavy wear and tear, potentially leading to crashes that could prevent them from being operational.

> Our biggest challenge was providing the flexibility for our teachers and students to create content and collaborate in innovative ways — while at the same time protecting information security in our distributed and complex environment."
>
> **Chris Paschke,** Director of Data Privacy and Security, Jefferson County School District, Colorado

Fighting Phishing, Outages, Cyberbullying and More

To solve these challenges, Jeffco turned to Splunk Enterprise and Splunk Security Essentials, which gave the school district a big-picture view of its environment and allowed it to resolve its security issues fast while keeping its network running reliably.

"The Splunk software takes event log data from multiple sources — such as our PeopleSoft management system and our firewalls — and delivers a comprehensive dashboard view that we use for analytics and forensic troubleshooting," Paschke says. "IT staff can type in a user's name and understand his or her activity on various systems. They can also track wireless connections, with anything unauthorized triggering a red alert."

With the Splunk platform, support center and service desk staff can now see and act quickly if a user clicks on a phishing link, steals credentials, or compromises an account. Paschke's team can track and verify employee password resets to protect against direct deposit fraud. They can triangulate device location within two meters, and track Chromebook device IDs and students associated with them if they've made threats.

To prevent the district's physical security monitoring devices from outages, the team now relies on Splunk Enterprise to monitor error codes and proactively alert staff, who can repair the hard drives before they crash to ensure uptime.

In addition, the Splunk platform also helps Jeffco address cyberbullying issues by allowing the team to track system usage, user and device access, as well as the times they were accessed. This capability, in turn, allows them to triage a post or threat that might be anonymous and track it down to a user or device. "The bullying often happens within an application that we don't have control over," Paschke says. Splunk helps us make sure that activity isn't anonymous on our network — that we have accountability if cyberbullying occurs."

Next Steps

With Splunk, Jeffco has already slashed mean time to resolution (MTTR) and aims to further reduce it to half an hour or less. The district also plans to increase security and logging around student grades & SIS data, as well as implement scripting and custom aids to automate processes, support field troubleshooting and guide escalations.

Down the road, Jeffco is also hoping to use Splunk software for proactive alert monitoring, as well as to improve IT system performance — particularly on test days — through predictive analytics.

20-15375-Tier2-Jeffco Public Schools-101-CS