

Derbyshire Fire & Rescue Saves Money and Lives by Maximizing Data

Key Challenges

Without a centralized log monitoring solution, the service's small IT team had poor visibility across system management, software updates and security threats.

Key Results

With Splunk, the small IT team improved security response and reduced cyber risk with better insights into the service's security posture, faster troubleshooting and enhanced collaboration.



Derbyshire
Fire & Rescue Service
Making Derbyshire Safer

Industry: Public Sector

Solutions:
Security, IT Operations

Derbyshire Fire and rescue Service is tasked with protecting more than a million people.

Providing prevention, protection and response throughout the county (which sprawls across 1,000 square miles), Derbyshire Fire and Rescue Service (DFRS) also stands ready to assist in national emergencies. Yet to deliver safety for citizens, the service must first ensure security for its 31 fire stations and two data centers, which were at risk of cyberattacks. Since it wasn't consolidating or maximizing the value of its data, the service was also missing valuable insights.

A New Approach to Data

Emergency response from DFRS saves lives and protects homes and businesses. Yet before adopting Splunk software, DFRS was battling a variety of internal risks. The service was harnessing little value from the data logs from IT systems and services. Operations were time-consuming and inefficient for the team — from not storing logs and running reports on an ad hoc basis to manually searching for details in event logs and security threats. And perhaps most critically, the service lacked a security incident and event management (SIEM) system.

When an external system provider mandated that the service have a SIEM as a condition of further collaboration, DFRS knew it was time for a change. The service chose the Data-to-Everything Platform over other options — including an offering from a software provider it was already using for other applications. “We tried a couple of Splunk demos online — one cloud-based, one on-premises — and it seemed a lot more intuitive to us,” recalls Pete Garyga, ICT security and project team manager for Derbyshire Fire & Rescue. Upon deployment, the Splunk platform immediately became valuable to day-to-day operations.

Turning Data Into Outcomes

- Blocked security intrusion before damage occurred
- Quickly spotted and repaired system maintenance issues
- Saved money by tracking and addressing printer misuse

Faster Workflows, Better Security, Smarter Decisions

Derbyshire Fire & Rescue is a small, hard-working team, with everyone performing multiple roles. Garyga, for example, is both security lead and project team manager. Since each worker's attention is split between tasks, saving time on one job frees resources for another. Splunk dashboards, which offer a visual overview of system health, have proved a welcome relief to busy staff. Previously, security incidents may have gone unnoticed with engineers having to manually trawl through log files to look for anomalies when something suspicious was identified. "With Splunk, any anomalies or issues that we need to identify are viewed quickly within seconds rather than several hours, and it's easy to drill down into the details," Garyga says.



Thanks to Splunk, we get vital information at a glance. It's helped us make better, more informed decisions."

Pete Garyga, ICT Security and Project Team Manager, Derbyshire Fire & Rescue



With Splunk, any anomalies or issues that we need to identify are viewed quickly, and it's easy to drill down and get into the details."

Pete Garyga, ICT Security and Project Team Manager, Derbyshire Fire & Rescue

The team now immediately spots trends or issues that need attention, bringing data to questions as varied as: Are the systems patched? Are firewalls properly configured? Are our internet-facing services being targeted? Are our web servers showing excessive errors? "Thanks to Splunk, we get vital information at a glance," Garyga says. "It's helped us make better, more informed decisions."

Splunk software has not only improved worker productivity — it's also helped the Fire & Rescue service avoid security disasters. "We've spotted intrusion events where we've blocked the source before anything damaging could have happened," says Garyga, who relies on the Splunk platform to perform his duties. "I look at Splunk hourly to see what's happening with our security posture. It's always on my right-hand monitor."

A Future of Cost Savings

Splunk technology has also put an end to costly printer misuse. The intuitive Splunk platform allowed the team to build their own Splunk App to provide dashboards, reports and alerts from a printing solution called Papercut. The app gathers information from daily log files and creates an automatic, monthly email report for department heads. By flagging overuse of printers or expensive tasks such as single-sided color copies, this report helps leadership turn data into action, helping save public money and improving the organization's policy on efficient use of shared resources.

DFRS expects the Splunk platform to enable more efficiencies and save even more public money. When the service carries out its planned migration to Microsoft Office 365, for example, the Splunk platform will monitor each user's license usage. This visibility will help the team identify if Microsoft's cloud service is being used across the organization and if DFRS has the correct license numbers. Finding the right balance will translate into better resource allocation and smart savings — helping Derbyshire Fire and Rescue protect and serve citizens with greater efficiency.

[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.



Learn more: www.splunk.com/asksales

www.splunk.com