Local UK Councils Collaborate Over Security and IT Operations to Improve Operational Efficiencies

Key Challenges

To better deliver local government services, Orbis needed to replace its antiquated legacy systems with one platform that retains separate data ownership while offering full visibility across the partnership.

Key Results

With Splunk, Orbis has created a single view of data across the three councils, improving collaboration and accelerating issue resolution while maintaining information governance.

orbis

Industry: Public Sector

Solutions: Security, IT Operations

Orbis has a big job on its hands.

The Orbis partnership was created to streamline back-office services across three local authorities in South East of England, comprising Brighton and Hove City, East Sussex and Surrey Councils. Spanning across 550 sites, Orbis delivers services such as finance, IT, procurement and HR to over 20,000 users.

Combining such a vast infrastructure meant a standardized security information and event management (SIEM) solution was essential to improve efficiencies and security. Splunk® has been a key part of Surrey County Council's infrastructure upgrade and modernization, which kick-started the SIEM replacement process.

Finding the Best Fit

The three councils within the Orbis partnership deliver local government services to end users at various locations, ranging from corporate management offices and fire stations to youth centers. Shrinking budgets had caused the councils to look at blending back-office systems as a way to improve efficiencies and reduce costs. However, diverged and disparate infrastructures made it hard for the security and networking teams to obtain an overarching view of compliance and IT operational needs.

Orbis member Surrey County Council had already chosen Splunk Enterprise as part of its own IT infrastructure modernization effort. Following a recommendation, the council chose Splunk ES as a natural fit to offer a standardized SIEM solution across all three councils, replacing existing products as they reached end of life or were deemed no longer fit for purpose.

Morgan Rees, technical delivery manager, Surrey County Council says, "Our desire within the partnership is to put everything on a converging basis but we must make sure that it's fit for purpose for each individual council. East Sussex was using a version of LogRhythm which was coming up to end of life, so they looked at what was on the market, and what Surrey was doing and saw that Splunk was the best fit."

Turning Data Into Outcomes

- Eliminated siloes and unified security visibility across 550 sites
- Secured information governance and compliance requirements that are critical to operating in the public sector
- Improved customer service through faster response times to faults and incidents

Comprehensive Operational Visibility

By replacing a raft of competing SIEM products and bringing that functionality under the umbrella of the Splunk platform, Orbis was able to achieve its desire of a single operational view while maintaining all-important information governance. “Splunk has allowed us to design and create three separate data stores for each organization and a common search head so that each council can maintain ownership or control over the data, and then using that common search head, data can be queried and searched to allow a centralized view and break down silos,” Rees says.

The Splunk platform also underpins Orbis’ adherence to various key compliance requirements by automating the collection, search, alerts and reporting of logs and machine data making it easier to build an audit trail. Of particular interest to Orbis was complying with Public Services Network (PSN) and National Health Service (NHS) regulations — crucial when handling vast quantities of the general public’s personal data or interacting with other government bodies.

> “There is a cost avoidance benefit by identifying security issues and incidents early, and quickly, that meant things like when WannaCry was hitting the NHS we could quickly identify where there were issues and remove the offending device from the network to prevent it from spreading further.”
>
> **Morgan Rees,** Technical Delivery Manager, Orbis

> “All compliance regimes require a good security practice, and that includes having a good SIEM tool that allows you to manage that risk with specific context to our organization. Splunk is a fundamental and underpinning part of those compliance regimes.”
>
> **Morgan Rees,** Technical Delivery Manager, Orbis

Improved Fault Resolution

Splunk Enterprise has been instrumental in speeding up fault diagnosis throughout IT services, including social care, waste and road management. According to Rees, cost avoidance through tool consolidation has been an unforeseen but greatly valued additional benefit to the original SIEM replacement function.

Using the indexed data gathered by Splunk, the network team has reduced the time taken to identify and respond to incidents ensuring improved customer service. Regardless of whether it is a security alert or troubleshooting website issues, multiple teams can now identify and resolve faults, limiting downtime and disruption as there is no need to go through multiple departments for escalations and root cause.

Ongoing Plans for Greater Improvements

By using Splunk Enterprise and Splunk Enterprise Security, Orbis has gained greater efficiency of services at scale and improved operational visibility. With public sector finances coming under increasing pressure, the partnership will continue to look for ways to capitalize on collaboration and sharing of information and services, according to Rees.

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>

Learn more: www.splunk.com/asksales

www.splunk.com