

Surrey Satellite Technology Enhances Ground Operations With Real-Time Infrastructure Visibility



Executive summary

Surrey Satellite Technology (SSTL) is the world's premier provider of operational and commercial satellites and aims to change the economics of space by making it more affordable to send satellites into orbit. To ensure that engineers and researchers had secure access to the IT tools they needed to further their work, SSTL required a solution that would help safeguard the uptime of key services. Since deploying Splunk Enterprise and Splunk IT Service Intelligence (ITSI), SSTL has seen benefits including:

- Enhanced ability to troubleshoot persistent service problems
- Improved security capabilities
- Greater visibility into overall IT performance

Why Splunk

SSTL was established in 1985 at the University of Surrey and became part of the Airbus Group in 2008, with a focus on producing satellites for the telecommunication, navigation and science markets. All employees having access to the right IT solutions to further research and development is crucial to the success of the business.

Prior to using Splunk Enterprise, SSTL did not have a consolidated view over its IT infrastructure nor its component tools, which meant that problems affecting applications or the network were difficult to address and resolve without periods of downtime. This lack of a single view was also having an impact on security. The siloed security solutions made security insights difficult to view in their full context. Through Splunk Enterprise and Splunk ITSI, SSTL now has centralized visibility over its core IT solutions, helping to troubleshoot problems, improve IT service levels as well as enhance security awareness.

Improved troubleshooting delivers research team benefits

Splunk Enterprise initially was used to help troubleshoot issues SSTL was having with its document management system (DMS). When there was a problem with the DMS system, the only way the support team could fix it was by logging out and then back in to the system. This meant that employees were losing access to documents for extended periods of time, affecting their research efforts. With Splunk Enterprise this process was no longer necessary, as issues could be identified and

Industry

- Technology

Splunk Use Cases

- IT operations
- Security

Challenges

- Difficulty troubleshooting problems within the complex document management system
- Lack of overall security awareness due to slow speed of existing search tools
- Inability to communicate IT performance to the rest of the business

Business Impact

- Rapid troubleshooting helps to ensure access to research resources for engineers and researchers
- Sophisticated monitoring and alerts have improved the overall security posture
- End-to-end monitoring of all IT services has ensured greater uptime of resources and delivered business visibility

Data Sources

- Syslog
- SNMP
- DB Input
- Stream
- Antenna logs
- Spacecraft logs
- Groundstation logs

Splunk Products

- Splunk Enterprise
- Splunk ITSI
- Splunk Technology Add-on for Microsoft Windows
- Splunk Technology Add-on for Unix and Linux
- Splunk Add-on for Bluecoat ProxySG
- Fortinet FortiGate Add-on for Splunk
- Splunk Add-on for Symantec Endpoint Protection
- Splunk Add-on for Infoblox
- Splunk App for ServiceNow

isolated without affecting usage of the entire system. Patterns of problems could also be identified and proactively addressed, improving overall stability.

Real-time visibility improves security capabilities

SSTL was unable to thoroughly investigate its security data, as its solutions all acted in a siloed manner. By using Splunk Enterprise to centrally store, index and provide insight into a range of data sources including firewall, Microsoft Active Directory, email hosting and website traffic, the organization now is able to rapidly search through data and establish alerts in a way that wasn't possible previously. This has improved the organization's ability to identify suspicious patterns that might point to security threats, with alerts established to recognize anomalies such as employees logging in at work when they haven't swiped into the office.

Insight into IT health and performance

Since deploying Splunk ITSI, SSTL has gained overarching insights into the performance of the organization's key services through a Service Health Score. Powerful visualizations provide easily digestible data and analytics in the form of dashboards that the business services team uses to better understand real-time performance

“Using Splunk Enterprise and Splunk ITSI has helped us to understand our IT network in a way we weren't able to previously. This has directly led to improvements in areas such as troubleshooting and security awareness, which is allowing us to focus more on how we can support our engineers and researchers.”

Daniel Nye, Chief Technology Officer
Surrey Satellite Technology

and business impact. This end-to-end view into IT highlights how potential problems such as a high load being exerted on the SQL server estate affects other key IT services. The team can then drill down into the data to accelerate root cause analysis and problem resolution. With Splunk ITSI, SSTL has been able to improve performance issues and ensure IT services are accessible, reliable and secure for all employees. “Using Splunk Enterprise and Splunk ITSI has helped us to understand our IT network in a way we weren't able to previously,” says Surrey Satellite Technology chief technology officer, Daniel Nye. “This has directly led to improvements in areas such as troubleshooting and security awareness, which is allowing us to focus more on how we can support our engineers and researchers.”

[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