CASE STUDY

Forschungszentrum Jülich Accelerates Problem Identification and Increases Efficiency

Executive summary

With more than 5,500 employees, the Forschungszentrum Jülich (Jülich Research Center) is a member of the Helmholtz Association of German Research Centers. Jülich's large campus IT network supports thousands of researchers and includes the Jülich Supercomputing Center (JSC), which provides scientists in Europe with computing resources of the highest performance class. Jülich needed a centralized log management system to enable faster, more comprehensive data analysis, alerting, reporting and compliance enforcement. Since deploying Splunk Enterprise, Jülich has seen benefits including:

- Real-time view of Operational Intelligence
- Reduced time to investigate and resolve issues
- Strengthened regulatory compliance

Why Splunk

The Jülich Supercomputing Center is home to JUQUEEN, one of the most powerful supercomputers in the world. In cooperation with known hardware and software providers, the JSC addresses the particular challenges that come with the development of next generation supercomputers. Jülich runs diverse IT-systems, with roughly 12,300 computers and up to 7,000 IP addresses permanently logged on to the network.

One of the biggest challenges the IT team faced was the large number of different authorization systems in operation. As a result, log data was not available in one central location, making any analysis extremely time- and resource- intensive for the security and network teams. Since they could not directly access the log data (firewall, DHCP and Radius), the teams were forced to request log data from IT administrators who then had to pull all relevant information from a myriad of systems. While several tools were in place to analyze the logs, they did not provide the desired holistic view.

The Forschungszentrum Jülich decided that a new, more efficient and secure solution had to be found: one that would serve as a central system for recording data and make it possible to define users'

Industry

- Technology

Splunk Use Cases

- IT operations
- Application delivery
- Security
- Compliance

Challenges

- Security and network teams needed centralized access to log data to accelerate troubleshooting and issue resolution
- Needed to gain greater control and coordination of access rights to supercomputers and other HPC systems
- Wanted to correlate and report on security alerts from internal and external sources

Business Impact

- Real-time and historical Operational Intelligence insight into huge volumes of log data from disparate sources
- Time and cost savings resulting from reduced manual workload through automated processes
- Reduced Mean Time To Investigate (MTTI) and the Mean Time To Resolve (MTTR) incidents, resulting in improved security
- Automated alerting and reporting has streamlined vulnerability management and strengthened regulatory compliance

Data Sources

- Firewall logs
- DHCP logs
- Radius logs
- CERT alerts

Splunk Products

- Splunk Enterprise
- Splunk for Cisco ASA App

roles with different access rights. The solution would need to be able to process large volumes of log data quickly and efficiently and guarantee correlation between the different log files, as well as automatically process events. Scalability was also an important factor, as data volumes are rapidly expanding. Bearing all these requirements in mind, the Jülich team deployed Splunk Enterprise.

Actionable insight achieved quickly

It took two research center staffers just two hours to set up Splunk Enterprise for an initial test. Within half a day, the first logs were being tracked and processed. Today, more than 2,000 syslog messages per second are processed with Splunk software. With user roles now corresponding to different access rights, security and network employees can easily access the data they need to get the job done. They can react immediately to security incidents such as a virus download, for instance, and can intervene before the impact is felt. The logs monitoring the authorized access to the operating supercomputer and cluster systems are now gathered and evaluated centrally. As a result, the Mean Time to Investigate (MTTI) and the Mean Time To Resolve (MTTR) issues have been drastically reduced.

Increased efficiency through automated alerting

From a strategic perspective, the research center also benefits from the introduction of Splunk software's automation capabilities. With Splunk Enterprise, automated alerts can be sent to certain groups of people. Through targeted communication with the responsible employee, vulnerabilities can be discovered more quickly and can be avoided when a certain threshold is exceeded.

> **"Splunk Enterprise enables us to easily capture and investigate logs from a number of different systems, all in one place. This flexibility coupled with reliable performance, even at scale, provides the Forschungszentrum Jülich with many valuable advantages: increased security and more efficient work processes."**
>
> Staff Member
>
> Forschungszentrum Jülich

In addition, regular security reports from the computer emergency response team portal of the German National Research and Education Network are automatically processed in Splunk Enterprise and compared against the center's own machine data. The research center also sees a further advantage in employing Splunk software for Operational Intelligence: now data can be processed or saved within the statutory retention period, enabling the center to adhere to strict compliance regulations.

Serving the needs of the research community

Splunk Enterprise has enabled Forschungszentrum Jülich to establish a strong centralized system for managing the vast amounts of machine data generated by the thousands of computers and other devices across the research campus. Searches and analyses conducted using Splunk Enterprise can now be saved and reused by authorized users, saving valuable time and accelerating the resolution of security and performance issues.

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