splunk> turn data into doing™

CASE STUDY

Lenovo China Improves Security Operations and Gains Actionable Insights With Splunk

Executive Summary

For over 35 years, customers and partners have relied on Lenovo for reliable, user-friendly technology and exceptional professional services. Generating an impressive RMB 342.2 billion — or US$51 billion — in 2018 alone, the global computer giant ranks number 22 on **Fortune's** 2019 Global 500 list and has more than 57,000 employees that span 15 research-and-development centers and 180 markets. As the company continues to scale, Lenovo needed an effective analytics tool to manage data growth and safeguard its operations. Since deploying Splunk Enterprise, Lenovo has:

- Maximized business agility through real-time log management
- Accelerated incident response with enhanced security monitoring
- Heightened operational efficiency

Security at scale

Gathering continuous streams of data from infrastructure logs, security software logs and application logs, Lenovo China generates two terabytes of data every day. With this ever-growing amount of distributed data, Lenovo needed a reliable solution for proactive monitoring and intelligent analytics that would allow the team to quickly identify and respond to security incidents.

Before Splunk, Lenovo's security engineers had to retrieve and correlate information from various system logs, then integrate and present the results in a visual format. Demanding hours of the engineers' time, this labor-intensive process made troubleshooting slow and complicated. If there was a virus infection, for example, engineers were forced to sift through numerous disparate terminal security platforms for relevant details before having to manually correlate all the data.

In search of a scalable platform for log management and security analytics, Lenovo evaluated the efficiency and cost-effectiveness of Splunk, ultimately choosing Splunk Enterprise for its stability, performance and ability to simplify system development.

Lenovo 联想

Industry

- Technology

Splunk Use Cases

- Log Management
- Security & Fraud

Challenges

- Low availability of data due to inflexible, labor-intensive log analysis
- Ineffective data monitoring and incident response
- Lack of intersystem data correlation to support security operations
- Inefficient management and retrieval of distributed IT data

Business Impact

- Improved security operations with automatic, real-time log management
- Increased reliability with faster threat prediction and timely incident response
- Boosted efficiency with accelerated application development and better use of employees' time

Data Sources

- Infrastructure logs
- Security equipment logs
- Security software logs

Splunk Products

- Splunk Enterprise

Real-time analytics with rich visualizations enhance decision-making

Thanks to Splunk, Lenovo China has streamlined workflows and improved productivity for a wide range of groups, allowing teams like application and security to work with greater agility and efficiency. In addition to enhancing data search, reporting, anomaly alert and security monitoring, Splunk also allows Lenovo China to seamlessly integrate different data sources for precise, real-time data retrieval and centralized monitoring and analytics.

With Splunk's easy-to-understand data visualizations, the team can efficiently turn complex data sets into real-time, actionable insights. These intelligent analytics have helped Lenovo unlock the power of its data, enhancing performance and enabling data-backed decision-making across the organization.

Unified data correlation increases efficiency and optimizes resources

From making daily tasks more efficient to bolstering security, Splunk has played a vital role in improving IT operations across Lenovo China. Requiring at least two technical staff to develop and integrate tasks, the company's previous open-source IT monitoring platform demanded considerable time, collaboration and interdepartmental communication. Splunk has eliminated these tedious tasks by aggregating, correlating and analyzing logs on a single platform — allowing employees to allocate their time to more strategic goals while saving money and better protecting the company from potential internal and external threats.

"The smart and reliable performance of the Splunk solution enables us to access real-time operational insights by extracting actionable information from raw data for detailed analyses and effective security monitoring. We are happy to have chosen Splunk and really look forward to a deeper partnership with Splunk in the future."

— Yu Sheng Li, IT Security Director, Lenovo China

Paving the way for a cloud-forward future

Splunk has enabled Lenovo to achieve new levels of success in its cloud migration journey. Previously, Lenovo was unable to solve deployment challenges when moving data and applications to the public cloud computing environment. Now with Splunk's reliable technology and real-time analytics, Lenovo quickly resolves any deployment issues that arise while easily collecting public cloud logs and streamlining application security logging.

Thanks to valuable insights from Splunk, Lenovo China will continue to sharpen its competitive edge, extending intelligent decision-making to every part of the business for an innovative future.

20-15687-SPLK-LenovoChinaImprovesSecurityOperations-103-CS