splunk>

CASE STUDY

Finanz Informatik Optimizes Risk Management With a Single SIEM Solution

finanz informatik

Executive summary

Finanz Informatik is the IT services provider to the 416 national savings banks, 18 regional banks or building societies, the DekaBank and several sub-contractors of the Sparkassen Finanz Gruppe. Its product offerings cover the entire IT spectrum—from the development and provision of IT applications, networks and technical infrastructure, to consulting, training and support. Finanz Informatik wanted to get an improved cross-platform view and analytics into its numerous environments. Since deploying Splunk Enterprise, Finanz Informatik has seen benefits including:

- Faster identification and investigation of incidents
- Reduced complexity, error rates and costs
- Better protection of customer data

Why Splunk

Finanz Informatik (FI) previously relied on different security information and event management (SIEM) solutions for its mainframe, network, Unix and Windows environments. To get an improved cross-platform view and analytics, Finanz Informatik wanted a single SIEM platform to be used companywide.

In addition to technical requirements, including data integrity, scalability, high availability and support, multi-platform security event correlation was of prime importance for Finanz Informatik. The new SIEM solution had to be capable of integrating seamlessly with its existing IT infrastructure and have multi-client capability. Now, the machine data generated by all the Finanz Informatik platforms is indexed and analyzed in Splunk Enterprise. This consists of data from several thousand machines, including servers, network and middleware components.

Industry

- Financial services

Splunk Use Cases

- Security

Challenges

- Better visibility across thousands of machines
- Spotting security events in real time
- Seamless integration of new SIEM with existing infrastructure

Business Impact

- A single cross-functional SIEM solution for faster and more comprehensive investigation and resolution of security incidents
- Better protection of customer data
- Operational visibility across multiple platforms

Data Sources

- Mainframe server logs
- Unix server logs
- Windows server logs
- Network logs
- Middleware component logs (e.g., databases and application servers)

Splunk Products

- Splunk Enterprise

Creating a comprehensive security information system

With its application OSPlus, Finanz Informatik provides the German banking sector with leading IT systems that execute 98 billion technical transactions each year. Subsidiaries including Finanz Informatik Technologie Service, Finanz Informatik Solutions Plus, Star Finanz and inasys round out the company's IT portfolio. The organization provides services for around 125 million accounts.

With Splunk Enterprise, FI can check—in real time or historically—how, when and where information and customer data was accessed, and by whom, across multiple platforms. FI has set up alerts in Splunk Enterprise that identify security events, authorization violations or unusual patterns of queries. The Splunk platform meets FI's requirements for a comprehensive security information system while also bringing added value in other use cases.

Increased security through faster identification and investigation of incidents

Finanz Informatik increased its security through faster investigation of incidents. Splunk Enterprise replaced the SIEM tools used before and offers FI a unified solution for comprehensive security information and event management.

Machine data analysis is now much easier. The existing data can be evaluated faster and across platforms for the identification and analysis of potential security incidents. With Splunk Enterprise as the basis of the new central SIEM solution, Finanz Informatik can better guarantee the full protection of its customer data and at the same time reduce complexity, error rates and costs.

"Splunk Enterprise is a well thought-out solution, designed from the outset for development and operation, and it delivers immediate results in a number of areas."

SIEM General Project Manager
Finanz Informatik GmbH & Co. KG