MICRO FOCUS | VERTICA

Customer Success Story

Vertica Data Analytics Platform
ArcSight Enterprise Security Manager

Finansbank

With Micro Focus® ArcSight and Vertica, the bank can identify anomalies more quickly, supporting more robust security and fraud-detection processes.

Challenge

For banks, trust is everything. Banks must win and retain the trust of their customers—consumers and businesses who turn to them for financial services.

Robust cybersecurity is therefore a bank's top business priority.

At Finansbank, the stakes are even higher. Founded in 1987, Finansbank is more than just a bank. It is one of Turkey's national institutions: its mission is to deliver the financial services that Turkish citizens and businesses need to catalyze Turkey's success.

To protect its systems against cybercrime and fraud, Finansbank has taken steps that most banks will recognize, such as deploying Micro Focus ArcSight Enterprise Security Manager (ESM) as its Security Information & Event Management (SIEM) solution. But Finansbank has also taken its cybersecurity capabilities a step further—by harnessing the power of big data analytics.

"Vertica lets us harness the power of big data to improve our "security capabilities."

ERDEM ALASEHIR
Consulting Security Designer
Finansbank

Solution

2-4 BILLION ROWS OF DATA

The bank's IT department owns a number of Micro Focus Software business process management solutions including Micro Focus Asset Manager, Service Management, Universal Configuration Management Database, Business Availability Center, Operations Manager, Data Center Automation and Business Service Management software.

The bank's security organization has a different set of needs. As people interact with Finansbank banking software, ArcSight ESM gathers data: over 120 Gbytes every day from around 15,000 data sources, totaling some 2–4 billion rows of information. This data, stored in Hadoop, represents a treasure trove of information and the bank needed to leverage it. It wanted to perform sophisticated SQL analytics to better understand the behavior of people who interact with its services, and to quickly determine what behaviors are benign and what behaviors are anomalous—and therefore potentially suspicious.

FINANSBANK

At a Glance

- **Industry**
  Financial Services
- **Location**
  Turkey
- **Challenge**
  The bank needed to enhance its cybersecurity capabilities.
- **Solution**
  Implement big data analytics software to facilitate high-speed baselining and profiling of user behaviors
- **Results**
  + Over 120 gigabytes gathered daily from 15,000 data sources
  + Performed queries on 2–4 billion data rows
  + Improved report generation
  + Empowered security team to quickly detect anomalies

"Vertica implementation facilitated the generation of compliance and audit reports. Formerly, the supply of bulk reports was a time and human consuming job, whereas it takes minutes now."

ERDEM ALASEHIR
Consulting Security Designer
Finansbank

www.microfocus.com

"We started to search for a strong, robust analytics solution to complement ArcSight ESM," explains Erdem Alasehir, Consulting Security Designer, Finansbank. "We thought at first we might use open-source software, but we discovered that the open-source options were not very user-friendly. Then we were introduced to the Vertica Data Analytics platform.

Results

When Finansbank expressed interest in Vertica, Micro Focus and the bank's security team set up a proof of concept (POC) to validate whether the software would meet the bank's needs, integrate with Hadoop, and support high-performance queries of the bank's ArcSight log files. The proof of concept was a success. "We were able to generate reports in a very short time," says Alasehir, noting that the team collected a billion rows of data during the proof of concept period. "We could immediately baseline data traffic and profiles, something that was not possible before we implemented Vertica."

The team also discovered that Vertica is easy to install and maintain. "We realized that the security department can run Vertica on our own, without needing the help of database analysts," Alasehir notes.

COMPLEX QUERIES IN MINUTES

Pleased with the successful POC, Finansbank deployed a production instance of Vertica. "Before, we had no way to work with the amount of data that we gather from our security software," Alasehir says. "But Vertica can handle it easily. And Vertica is fast: we can run complex SQL queries in a couple of minutes. We also develop python middleware to automate reports, or make computations and update near real-time profile tables also kept on Vertica. They work perfect together."

This speed is critical, because it enables the bank to react more quickly to anomalies that might represent malicious or fraudulent behaviors. This gives the bank a valuable edge in its cybersecurity battle. Cyber threats are continually evolving: as businesses work to neutralize existing cybersecurity schemes, hackers and fraudsters are seeking new vulnerabilities to exploit. Finansbank, by acquiring the capability to perform complex modeling quickly, is better positioned to stay a step ahead of these vulnerabilities.

"With a fast and robust database, you are limited only by your imagination," Alasehir concludes. "We are tremendously satisfied with the way Vertica has extended our cybersecurity capabilities, not only the performance aspect but also ease of integration and creation of use cases."

Micro Focus
UK Headquarters
United Kingdom
+44 (0) 1635 565200

U.S. Headquarters
Rockville, Maryland
301 838 5000
877 772 4450

Additional contact information and office locations:
www.microfocus.com

Learn more at: **Vertica.com**

VERTICA | MICRO FOCUS