NXLog

# NXLog Empowers QNB Finansbank with a Robust Security Telemetry Pipeline

QNB

## CUSTOMER PROFILE

QNB Finansbank, originally founded as Finansbank A.Ş. on October 26, 1987, became the first private bank in Turkey to go public. In June 2016, it was acquired by Qatar National Bank S.A.Q. (QNB Group), the largest bank in Qatar and a leading financial institution in the Middle East and Africa. Today, QNB Group operates in over 1,100 locations and has a network of more than 4,300 ATMs. In 2023, QNB Finansbank achieved a net profit of TRY 33.17 billion. As of December 31, 2023, the bank has 436 branches and employs 11,756 individuals.

## RELATED INDUSTRIES

- Consumer Banking
- SME/SMB Banking
- Corporate Banking
- Private Banking
- e-Finance

## BUSINESS DEMAND

Enhance cybersecurity and operations monitoring to strengthen security posture and ensure greater system resilience.

## CHALLENGES

Build a unified log collection pipeline to aggregate events from various sources, including thousands of ATMs across branch offices. Minimize the load on the SIEM by filtering and processing data efficiently. Ensure seamless routing of logs to both security systems and the general-purpose data lake.

## SOLUTION

- NXLog Platform
- NXLog Professional Services

## BUSINESS RESULTS

- A unified telemetry pipeline has been successfully implemented
- Security posture enhanced through comprehensive log collection coverage
- The operations team now leverages log data from the data lake for improved insights and decision-making

NXLog

# NXLog Empowers QNB Finansbank with a Robust Security Telemetry Pipeline

## BACKGROUND

According to IBM, the average cost of a data breach reached an all-time high of USD $4.45 million in 2023, marking a 2.3% increase from the previous year's cost of USD $4.35 million. Over the long term, the average cost has risen by 15.3% from USD $3.86 million in 2020. Alongside healthcare, the financial sector tops the list, with an average breach cost of USD $5.90 million. Additionally, the mean time to identify and contain a breach has now reached 277 days.

Notably, breaches identified by an organization's own security teams and tools are significantly less expensive — nearly USD $1 million less — than those disclosed by the attacking parties. To reduce detection time and mitigate costs, implementing effective security log management is essential. Research has shown that 27 factors impact the average cost of a breach, with half of the cost mitigators relying heavily on log collection, including SIEM/SOAR systems, DevSecOps processes, incident response, threat hunting, and AI/machine learning-driven insights.

For financial institutions, particularly those with rapidly expanding infrastructures and large attack surfaces, establishing a robust log collection (telemetry) pipeline is critical. This is especially true for IBTech service provider, founded by QNB Finansbank, which manages the full cycle of R&D, infrastructure, and cybersecurity operations for QNB Finansbank and its subsidiaries.

## SOLUTION

To maintain a comprehensive and consistent defense-in-depth, IBTech's security team must collect logs across hundreds of QNB Finansbank branches and a wide range of endpoints, including office computers, servers, and network equipment. For QNB, each endpoint generates a diverse array of log types, such as Windows, macOS, and Linux operating system logs, application logs, antivirus events, EDR logs, PowerShell logs, Sysmon logs, and others critical for both real-time and on-demand analysis.

QNB Finansbank also operates an extensive ATM network with thousands of cash dispensers from various vendors, each generating important security log data. Given the critical role of these ATMs in daily operations, the entire network must be covered by log collection.

In line with their security policy, all valuable log data must be continuously collected, filtered (to avoid network and storage overload), normalized to specific schemas, and sent to multiple destinations, including security systems (SIEM, UEBA) and operational analysis tools (general-purpose data lake). Collecting logs from disparate sources typically requires a range of different tools, complicating the process and introducing several potential points of failure. To simplify and streamline this process, IBTech needed a unified, autonomous log collection pipeline (telemetry pipeline).

After evaluating several options, NXLog Platform was selected for its versatility, powerful data transformation capabilities, and extensive integration options. NXLog agent was successfully deployed across more than 15,000 endpoints within weeks and seamlessly integrated with the SIEM solution.

IBTech's security team adopted a hybrid log collection strategy, using NXLog agents installed locally on endpoints and deployed on the network as remote log collectors (agentless mode). A strict data filtration policy was applied to ensure only necessary data was ingested into security systems like SIEM and UEBA, optimizing the performance of the bank's security operations.

*The entire telemetry pipeline becomes both powerful and easy to maintain with NXLog. We value its high level of configurability and advanced log processing engine, which enables us to filter out up to 80% of events directly at the endpoints. This ensures that only the most relevant data is fed into our security systems, streamlining security operations*

*One of our main challenges was enabling log collection across branch offices and the ATM network. NXLog offered a variety of integration options with diverse data sources, allowing us to build a flexible and robust log collection architecture that effectively supports both our security and operations teams.*

Ahmet Uygut, Expert Architect,
IBTech Security Incident
Management and Monitoring

For more information about NXLog products and services, visit our website,contact us via the web form, or schedule a meeting.

Start free with the NXLog Platform now!