



Data Protection Helps QNB Finansbank's Information Security Department Manager and Five Million Customers Sleep Better at Night

This top-five Turkish bank is safeguarding its brand, reputation, and customer information with Forcepoint DLP, and its Security Incident Management leader wouldn't have it any other way.

Turkey's economic growth and a steadily increasing population have created increased demand for personal banking services. In this highly competitive environment, QNB Finansbank has become one of the country's five largest financial institutions by delivering on its mission of "establishing a lifelong partnership with stakeholders" and "aiming for maximum customer satisfaction." Management knows that the bank's reputation is everything, and a violation of customer data—and customer trust—would be catastrophic.

CUSTOMER PROFILE:

Established in 1987, QNB Finansbank is one of Turkey's top five largest banks. This dynamic, multi-award-winning financial institution has more than 500 branches and 12,000 employees.

INDUSTRY:

Banking

HQ COUNTRY:

Turkey

PRODUCT:

Forcepoint DLP

As organizations grow and expand, so do vulnerabilities. And financial institutions continue to be prime cyber targets. The potential for damage was real enough to keep QNB Finansbank's Information Security Department Manager, Ahmet Taskeser, up at night. "The most important thing that we are trying to protect is the reputation of Finansbank, which is priceless for us," said Taskeser.

The business hinges on protecting the bank's more than 5 million customer account numbers, credit card data, and security tokens from inbound attacks like advanced persistent threats, malware, and phishing emails.

But it wasn't just inbound threats that Taskeser worried about. He was increasingly aware of inside threats and their potential damage—whether through accidental or malicious actions. A McKinsey & Company examination of the VERIS Community Database, for example, showed that about half of publicly reported breaches from 2012-2017 had a "substantial insider¹ component." Internal employees, often unwittingly, are a weak link in the system.

"Upper management are very happy about this high level of quality from Forcepoint."

AHMET TASKESER, INFORMATION SECURITY DEPARTMENT MANAGER

Regardless of the source, a successful data breach can have widespread effects that could not only negatively impact its depositors and financial partners, but also severely damage—if not destroy—the bank's brand.

That's why QNB Finansbank sought to implement additional measures into its security stack. To keep up with an ever-growing number of potential inbound and outbound vulnerabilities, it needed a powerful but versatile security solution to guard against data leakage without disrupting the organization. Which is why QNB Finansbank turned to Forcepoint.

Up and running in two days, with no additional servers

Installation and product configuration can be a very complex process with competitor software, but QNB Finansbank found Forcepoint's process seamless. With the support of Forcepoint engineers, they were able to install Forcepoint DLP in just two days.

"Forcepoint's deployment was much more streamlined than its competitors'. We didn't need to add servers to deploy its security solutions, while others would have required us to add as many as 12 servers," said Taskeser. "One Forcepoint engineer came in and, after two days, everything was ready and we were detecting all incidents on my screen—which was unbelievable. This, coupled with the expertise and exceptional support from the Forcepoint engineers, made the decision to go with Forcepoint very simple for us."

After deploying Forcepoint DLP, QNB Finansbank was able to achieve a more detailed, comprehensive look at how the bank's 12,000 employees—across retail branches, operations, and corporate headquarters—access and interact with sensitive information. Becoming more attuned to how people and data interact enabled Finansbank to better address both inbound and outbound data vulnerabilities.



Challenge

Safeguarding account data for 5 million customers in order to maintain brand reputation.



Approach

Deploy Data Loss Prevention (DLP) to provide detailed visibility into how 12,000 employees access and interact with sensitive information.

¹ <https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyber-risk>

Becoming one of the world's 50 safest banks

QNB Finansbank saw results right away, from improved insider threat controls to significant reductions in the resources required to maintain an effective data security program.

Finansbank was able to identify risky users much faster, with drastically reduced false positives. And data fingerprinting capabilities mean that Taskeser and his team can follow their data even when user devices are off-network. All these features and more allow the security team to be more attentive to potential issues, understand what's really important, and respond more quickly.

"We had an issue with an employee. He was trying to gain access to some customer data but was prevented from doing so using Forcepoint DLP," recounted Taskeser. "I wasn't expecting Forcepoint to detect such a detailed test, but it did. Upper management are very happy about this high level of quality." The bank has since been ranked as one of the top 50 safest banks in the world by Global Finance Magazine.

QNB Finansbank was also able to cut costs by optimizing staff resources, Taskeser said. "Before Forcepoint, we had four employees who were devoted to reviewing highly secure documents before they were sent to auditing companies. Now Forcepoint does the reviewing for us," he said. Taskeser has also found management of Forcepoint's solution to be easy—everything is tuned from just one interface.



10+

years of partnership



02

days to implement incident detection

Incident response times shrink from days to hours

Forcepoint's long-term partnership with QNB Finansbank actively supports the bank's security journey with regular check-ins regarding organizational needs and product performance health.

Over the last 10-plus years, QNB Finansbank has come to see Forcepoint as a trusted partner in its security journey, including the development of a connection between each company's C-level leadership, with senior leaders calling each other directly to discuss security challenges.

"I sleep better at night knowing that our data is secure with Forcepoint."

AHMET TASKESER, INFORMATION SECURITY DEPARTMENT MANAGER

In preparing for the next step of its security journey, the bank is currently working with Forcepoint on a proof of concept for Behavioral Analytics. This solution can integrate with DLP to use Forcepoint's deep understanding of human behavior and intent to enable greater automation and faster incident response times—from days down to hours.

A proactive and humanly attuned approach dramatically improved QNB Finansbank's protection of critical data. The organization is confident in its ability to secure its customers within a trusted environment—which gives Taskeser the greatest reward of all: "I sleep better at night knowing that our data is secure with Forcepoint."



Results

Incident detection implemented in just two days.

Eliminated need for employees to handle pre-audit document reviews, cutting costs.

Reduced false positives and facilitated faster incident response times (days to hours).

More than a 10-year partnership.