CUSTOMER STORY

FireEye

# Major Turkish Bank

## Stopping Attackers in Their Tracks: A Turkish Bank Improves Threat Intelligence with FireEye

**FACTS AT A GLANCE**

**INDUSTRY**

Financial Services

**SOLUTIONS**

Multiple FireEye Solutions

**BENEFITS**

Unified on-premise security infrastructure

Automated threat analysis drastically reduces false positives

Data privacy compliance with on-premise security infrastructure

Real-time exchange of threat intelligence across attack vectors improves overall security effectiveness

Visibility into attacker intent, activity and tactics enables a quicker, more targeted threat response

**CUSTOMER PROFILE**
This financial institution is a commercial and consumer banking organization, serving millions of customers at hundreds of branches across Turkey.

With millions of customers, the bank has millions of reasons to maintain impregnable defenses capable of protecting the enormous amount of personal data stored by the financial organization.

Building a highly tailored security program was vital to protecting the bank from a regional cyber security landscape rife with threats. The incident response and threat intelligence unit manager for the bank's Cyber Defense Center, expounded on the challenges he and his colleaugues face: "There are several infamous regional and global groups that constantly attack the financial institutions in Turkey. These cyber criminals have become very skilled at varying their tactics and are leveraging increasingly advanced malware to execute their assaults. In Turkey, sophisticated forms of phishing have been their attack vector of choice."

As a key part of the bank's security strategy, the Cyber Defense Center team is responsible not only for analyzing and responding to attacks on the bank, but managing threat intelligence analysis and strenghtening incident detection rules and scenarios.

> "FireEye knows our country well, understanding the specific risks we face and how to handle them."
>
> — Incident Response and Threat Intelligence Unit Manager, major Turkish bank

Aside from fortifying defenses against highly organized and well-funded groups of threat actors, the bank needed a security solution to both conform to Turkey's data privacy laws and complement the extensive expertise of the incident response and threat intelligence unit.

The unit manager elaborated on his requirements, "In Turkey, we have rigorous banking regulations that restrict the use of cloud-based applications for handling customer data. In addition to operating exclusively with an on-premise infrastructure, there is the regional challenge of identifying qualified security professionals with the appropriate level of field experience and technical knowledge to protect our environment from the constantly changing trends in cyber security."

## Dynamic Protection for Each Attack Vector

In order to safely evolve its carefully architected security infrastructure, the bank rigorously evaluates potential solutions before adopting any new technology. The unit manager described, "When we are interested in deploying a new service or product, we put the candidate solution in a test environment to conduct an intensive proof-of-concept [POC]. During this process we measure the technology's performance by grading each of the capabilities that are relevant to us, and comprehensively analyze the findings to identify the solution best-suited to our environment."

After conducting POCs on several leading security components, the bank determined that a suite of FireEye solutions would provide the strongest approach to secure key attack vectors. The deployment resulted in improved protection throughout its distributed environment. Collectively, the solutions generate actionable, adversary-focused context on threats that help improve defenses against the tactics, techniques and procedures (TTPs) of probable attackers.

"When one of the FireEye solutions detects a threat, intelligence is exchanged with the other solutions to ensure that each is appropriately prepared for the attack," the unit manager enthused.

## Contextual Threat Intelligence for Adaptive Defenses

The threat intelligence unit at the bank values the accuracy and agility of the FireEye solutions. Since their deployment, the operational efficiency of its security infrastructure, and consequently the threat intelligence team, has drastically improved.

"I'm very satisfied with the low false positive rate of the FireEye solutions. Each one uses automated threat analysis, which is an important benefit in our region where most companies – our bank included – often don't have enough resources to analyze all the suspicious activity that is occurring," attested the unit manager. "FireEye enables us to quickly identify an attacker's intent, tactics and activity. We are able to continuously adapt to be prepared for the newest emerging tactics of hackers."

The FireEye support team has been available as a resource for the bank throughout deployment and implementation. The unit manager recounted, "The local FireEye office has worked closely with us every time we've had a question about the solutions. Whether it's a FireEye software engineer or support staff responding to our inquiries, they've always quickly delivered the answers we've needed."

## Confidence Comes with Experience

Summarizing his confidence in the bank's FireEye solutions, the unit manager shared, "For our bank in Turkey, seeking services from a cyber security company with first-hand experience working in our region is critical. FireEye knows our country well, understanding the specific risks we face and how to handle them."

To learn more about FireEye, visit: **www.FireEye.com**

**FireEye, Inc.**
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com



**About FireEye, Inc.**

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks. FireEye has over 6,600 customers across 67 countries, including more than 45 percent of the Forbes Global 2000.

FireEye®