Forcepoint

Customer Story

VAKIFBANK Strengthens Security Posture and Compliance Reporting

VAKIFBANK leveraged pre-defined policies in combination with fingerprinting and a third-party classification tool to protect tens of millions of customer records and improve compliance.

Banking and consumer privacy regulations drove VAKIFBANK to implement Data Loss Prevention to protect the personal information of its 15 million customers. After deploying the solution in just one month, the institution leveraged out-of-the-box policies, fingerprinting, and a third-party classification tool to discover and protect nearly 20 million files. VAKIFBANK blocked 4,000 incidents within the first three months and now manages nearly 50 policies.

VakıfBank

CUSTOMER PROFILE:
Established in 1954, VAKIFBANK is the second-largest bank in Turkey with nearly $50 billion assets under management. The bank's products and services extend across commercial and retail and can be accessed online or through its over 900 branches. The firm also has offices in the U.S., Qatar, Bahrain, and Austria.

INDUSTRY:
Banking

HQ COUNTRY:
Turkey

PRODUCT(S):
› Data Loss Prevention (DLP)

Compliance Motivates Security

Information security is everyone's responsibility at VAKIFBANK. The second-largest bank in Turkey has over 15 million customers and the Personally Identifiable Information (PII) and Personally Identifiable Financial Information (PIFI) it holds extends to most of the families in the region.

Combine that responsibility with its presence across the globe, and it's easy to see why VAKIFBANK takes data security so seriously.

An audit in 2012 from the Banking Regulation and Supervision Agency of Turkey spurred the institution to review its data security strategy. At that time, it lacked the products to monitor information within its database, track how that information flows through and out of the organization, and provide visibility to auditors of its information security practices.

"The motivation behind moving to Forcepoint was data privacy – GDPR and KVKK being the two big reasons," Akif Mert Avcı, Information Security Manager, said.

Avcı and his colleague Elif Ahmetoğlu, Technical Manager of Information Security, sought a solution that would make compliance simple, ensure that information security was accessible to all the teams who needed to report such as Human Resources or Finance, and provide the security controls necessary to safeguard data.

Simplifying Data Security

VAKIFBANK tested three different Data Loss Prevention (DLP) platforms, but only one stood out: Forcepoint.

A strong selling point for Forcepoint DLP was the pre-defined policies that security administrators can use to automatically adhere to regulations such as the General Data Protection Regulation (GDPR) and the Turkish data privacy law, KVKK.

The institution also appreciated the ability of Forcepoint DLP to automate third-party data classification tools, which it needed to comply with GDPR. Without the DLP, classification would be a time-intensive process.

Deploying the DLP platform and installing 17,000 endpoint agents took Ahmetoğlu and team only three months from start to finish. The bank implemented 49 data protection policies, with nine of them dedicated to GDPR and KVKK.

The management console lends itself to end users with various levels of experience, Other business units were able to quickly learn how to use the platform for investigations and reporting.

Once the platform was up and running, VAKIFBANK spent considerable time using Optical Character Recognition (OCR) fingerprinting – especially for data that wasn't used over a certain period.

"Fingerprinting helps greatly with our fraud investigations, and it also enables us to figure out what data isn't being used so we can act accordingly," Avcı said.

VAKIFBANK also uses DLP blocking mode for certain incidents, categorizing them into three categories: low, medium, and high-risk.

Challenge

- Comply with GDPR, KVKK, and safeguard the PII of corporate and personal banking accounts.
- Secure the various IP and critical assets.
- Protect data from threat actors and secure it from being exported or sent via email, web, and endpoint channels.
- Discover, classify, monitor, and defend data across all endpoints, database, and file sharing platforms.

Approach

- Deploy Forcepoint Data Loss Prevention (DLP) in one month.
- Implement almost 50 different data protection policy templates.
- Turn on monitoring and fingerprint nearly 20 million records.
- Accelerate time-to-value of third-party classification tool through Forcepoint DLP automation.

While high-risk incidents are blocked by default, the team intervenes in medium and low-risk incidents. One example of this is to initially block an email containing sensitive information, educate the user on why it's blocked, and investigate the incident to determine whether the information can be sent. Ahmetoğlu and Avcı believe this process is improving information security awareness within the business.

Driving Value for the Business

After the first three months of running Forcepoint DLP, VAKIFBANK was able to block 4,000 incidents. The situations spanned emails, documents, and other ways of sharing sensitive data.

Since then, VAKIFBANK has either classified or fingerprinted nearly 20 million files. The institution finds it easy to implement end user policies, ensuring gets the most accurate protection possible.

"We have around 20 different products we use for data security but the tool we like the most is DLP," Avcı said. "As time changes, data becomes more valuable, and we must protect this data from leakage. DLP makes reducing our risk very easy and adds the most value to the company."

Forcepoint DLP succeeded in making compliance easier. Not only do all the teams use the platform for their own auditing needs, but the policies and reporting provide an excellent source of truth for external auditors.

While Forcepoint DLP has had a role in the success of VAKIFBANK, success is also attributed to the generous support from the top levels of the organization.

"We can't create and implement policies in the dark – there needs to be collaboration with business leaders," Avcı said. Especially our General Manager Abdi Serdar ÜSTÜNSALİH, the support we receive from his leadership makes it much easier to implement these policies, achieve compliance, and ensure we secure customers' sensitive information."

The financial institution also enjoys speedy resolution times when it has issues that need to be resolved with the tool. "If there's an issue, we can easily contact our Forcepoint team," Avcı said. "We don't get this support response speed with any of our other products."

Moving forward, VAKIFBANK is looking to take advantage of the new developments and features in DLP technology. One area includes machine learning, which will make it easier for the information security team to adapt policies to user behavior or unique circumstances.

"We plan to implement Risk Adaptive Protection because it will give us more versatility to apply real-time protection to user behavior," Ahmetoğlu said. "When we set a policy, it's the same for all clients and users. We'd like to adjust it on an individual basis for, as an example, anomalies or higher access levels."

Results

- Comply with all major regulatory concerns across the globe.
- Secure PII, PIFI of its more than 15 million customers.
- Fully automate labelling of data for quicker classification.
- Consolidate policies for greater efficiency and seamless management.
- Enable identification of any high-risk users that mishandle critical data.
- Improve security awareness of departments through user education.
- Provide visibility into events and timelines involved in a data breach.
- Identify personal data using OCR capabilities to detect text within images.