
# VakıfBank

## Endpoint Security Reduces Attack Surface for Leading Turkish Bank

**Industry**
Banking

**Challenge**
Reduce impact of attacks by strengthening endpoint security for 17,000 employees

**Solution**
Palo Alto Networks Traps to preemptively block both known and unknown threats

**Results**

- Reduced attack surface by strengthening endpoints
- Delivered data to enable analysis of new threats
- Provided visibility of threat landscape
- Secured PCs for 17,000 employees

VakıfBank is one of the biggest banks in Turkey. It has 924 branches, 3,917 ATMs and approximately 16,000 employees, and plays an important part in financing the country's domestic and commercial trade. In addition, it has operations in New York, Bahrain, Germany and Austria.

"Cyberattacks on the Turkish financial sector are increasing year over year," says Evrim Eroğlu, Head of Security Infrastructure Operations for VafikBank. "No environment is 100% secure, but we can reduce the surface of attack. Our intention is to focus on the weakest point in the chain: our endpoints."

Endpoints matter, he says, because with employees becoming more mobile in their work culture, laptops are used off the network: "Staff use their own PCs at home. Protecting our own network wouldn't be enough to keep us secure."

Eroğlu's contention is that traditional signature-based security is not enough to protect against the variety of attacks faced by a modern bank: "They are incapable of detecting or protecting against zero-day attacks."

The bank created a proof of concept to review options from leading security solutions providers, testing against 100 known malware variants. "We tested several products," says Eroglu. "McAfee, Comodo, FireEye, Carbon Black, Trend Micro, Check Point … none of them were able to detect and stop this kind of attack. Traditional antivirus security was not the solution. We were using McAfee Endpoint Security, and it wasn't able to detect every threat (zero-day attacks). Only Traps from Palo Alto Networks worked."

Traps will replace AV with multi-method prevention: a proprietary combination of malware and exploit prevention methods that preemptively block both known and unknown threats.

The PoC was carried out through the summer of 2016. The rollout of Traps to 17,000 VakıfBank PCs started in October.

> “We’ve seen the benefits from day one, even before the rollout was fully completed. We’re certainly more secure as a result of Traps.”
>
> **Evrim Eroğlu** | Head of Security Infrastructure Operations | VakıfBank

“We’ve had to be careful with the rollout, testing at every stage,” says Eroğlu. “We wanted to be sure there was no impact on any of our critical business applications. We had issues with other solutions during the PoC, slowing the performance of PCs. That hasn’t happened with Traps.

“It was important we had a cautious, planned and smooth rollout of Traps. We started with 50 PCs, then 100, then 1,000, and another 1,000, then 5,000. At every stage, where there were concerns, Palo Alto Networks addressed them.”

### Analyzing the threat landscape

Traps, says Eroğlu, protects and detects, and provides the information his team needs to follow up on and analyze new threats. “We’ve seen the benefits from day one, even before the rollout was fully completed. We’re certainly more secure as a result of Traps, but we remain vigilant.

“The threats keep coming. What’s invaluable about the Palo Alto Networks offering is that we now have more data through which to forensically examine threats and their potential impact.”

The introduction of Traps will enable VakıfBank to make cost savings as it allows its McAfee licences to expire over the next two years. However, Eroğlu says extra investigative work means it is unlikely the operational costs of security will come down. The smooth implementation of Traps, and its immediate effectiveness, have encouraged a greater appetite for tackling security. The bank is planning a new Security Operations Center.

“We don’t just want to react to threats as they arrive; we want to see them coming. We have to work harder than ever. Traps means we see new malware and we have greater visibility. Now, the challenge for us is to switch from being reactive to proactive,” concludes Eroğlu.