FireEye®
SECURITY REIMAGINED

# Bank of Thailand chooses FireEye technology to manage advanced protection

CUSTOMER STORY

SECURITY
REIMAGINED

## KEY COMPONENTS

- FireEye® Network Threat Prevention Platform
- FireEye® Email Threat Prevention Platform
- FireEye® Central Management
- FireEye® Threat Intelligence

As a major economic institution in one of the growing regions of the world, the central bank relies on an IT infrastructure that is capable of handling a variety of demands and issues.  Keeping up with the latest cybersecurity advances and challenges is needed to keep the organization secured.

New threats, increasing in volume and sophistication, are designed to go undetected for long periods of time and require a technology capable of detecting attacks that traditional cyber defenses miss. They require a new far-seeing cybersecurity strategy and the right tools to support this strategy.

| COMPANY | Bank of Thailand |
|---|---|
| INDUSTRY | State Enterprise/Finance |
| DESCRIPTION | Key roles of the Bank of Thailand are formulating monetary policy and promoting monetary stability, managing the money supply in the financial system, printing and issuing bank notes, establishing and supporting payment systems, and providing banking facilities for financial institutions. |
| CHALLENGES | • Staying ahead of issues that could endanger the bank's mission<br>• Identifying and blocking unknown cyber threats that are missed by traditional defenses<br>• Preventing the potential compromise of critical operations and data |
| SOLUTION | • FireEye Network Threat Prevention platform<br>• FireEye Email Threat Prevention platform<br>• FireEye Central Management<br>• FireEye Threat Intelligence |
| BENEFITS | • Heightened visibility of threats<br>• System-wide monitoring<br>• Enhanced institutional awareness around advanced persistent threats (APTs)<br>• Rapid identification and response to a range of cyber threats |

BANK OF THAILAND

> "Best practice is no longer good enough when it comes to cybersecurity. The world has changed dramatically. The reality of what we face is a world with an extraordinary array of new security challenges. From proof of value to implementation, Bank of Thailand chose FireEye technology to manage advanced protection."
>
> — **Senior Director,** Information Technology Department

## PROOF OF VALUE LEADS TO DISCOVERY AND IMPLEMENTATION

Entrusted with promoting a stable financial environment to achieve sustainable and inclusive economic development, the central bank is an institution whose mission is extremely sensitive and whose reputation is critical.

At the core of the bank's ability to meet its mandate is a substantial IT infrastructure that not only needs to run optimally, but must be protected. The bank had long embraced best practices when it came to cybersecurity, but recognized that advanced threats evolve over time and need to be well handled.

Guided by a trusted technical advisor, the bank selected FireEye for a proof of value (POV) conducted over a period of three months. The POV soon discovered a number of previously undetected threats enabling system administrators to take action and make the system even more secure.

As a result of the findings, the bank implemented FireEye to strengthen their IT infrastructure. This solution consists of FireEye Network Threat Prevention platform and FireEye Email Threat Prevention platform in operation alongside FireEye Central Management to coordinate intelligence gathering from the Web and email appliances in addition to the intelligence gathered by the FireEye Threat Intelligence.

## BEST PRACTICES BECOME BETTER WITH FIREEYE

The central bank followed best practice when it came to cybersecurity, but like many organizations with a global profile and substantial national responsibilities, the IT leadership team understood that this wasn't enough anymore. This view was reinforced when FireEye briefed the bank's cybersecurity team on APTs prior to the POV.

The POV was up and running in less than a day and used actual traffic analysis to investigate what was occurring in the bank's IT environment. According to the senior director of the bank's Information Technology department, "the POV quickly revealed areas for improvement and potential threats that the traditional defenses had utterly missed."

The FireEye team remained in close contact with the bank's key personnel throughout the process. As the senior director said, "FireEye proved very supportive both of the technical and business aspects of the POV and ultimately our implementation of their technology both in terms of cost and underscoring the difference between traditional defenses and the next-generation defense system."

Looking ahead, the Bank of Thailand is continually strengthening their IT infrastructure together with reinforcing policy and process on IT Security to achieve the highest productivity and lowest risks.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**

FireEye