FireEye®

Protecting Australia's Police Bank from Criminals

policebank
member owned banking

FACTS AT A GLANCE

INDUSTRY

$ Finance

CUSTOMER PROFILE

Founded in 1964 by a group of Police Officers in Sydney, Australia, Police Bank has grown to become one of the country's largest and most successful mutual financial institutions. With total assets exceeding AUS$1.6B (US$1.2B) and over 70,000 members, Police Bank has won multiple awards for its products, low rates and customer satisfaction. Membership is open to the Police Family Community including employees of local agencies, relatives and associates broadly involved with law enforcement and emergency services.

Police Bank offers its Members a wide variety of highly competitive financial products, including savings, loans, insurance and financial planning.

"With the word 'Police' in our name, security always has to be a priority for us!" remarked Paul Klauzner, Police Bank's Chief Information Officer. To deliver on expectations and to ensure that the Bank's assets are continually protected, Klauzner performs regular risk management assessments across his organisation's entire IT environment.

"We assess potential vulnerabilities from a wide range of threat vectors and use the findings to create appropriate mitigation strategies. We don't have a large security team, and with the escalating volumes and sophistication of cyber attacks, it became clear that we needed to deploy additional capabilities," recalled Klauzner.

The Bank issued a request for proposal to solicit input from multiple security providers: "A common theme across a number of the proposals was an unrealistic requirement to add more headcount. Pricing was another hurdle that helped us narrow the pool of candidates further."

"Knowing that we have FaaS handling the really sophisticated attacks gives me the time to focus on other key areas of my job."

— **Peyman Gohari,** Head of Security, Police Bank

Protection with the right coverage

Klauzner and Police Bank have had a longstanding relationship with Optus, an Australia-based IT services, hardware and consulting provider. Optus recommended the implementation of FireEye® as a Service (FaaS) to address the Bank's immediate requirements: "FaaS was financially beneficial, and it delivered exactly the coverage and functionality we needed," commented Klauzner.

He added, "Prior to subscribing to FaaS we had several conversations with colleagues in the federal cyber crime division and the level of endorsement we received for FireEye solutions persuaded us that we should move quickly to implement FireEye as a Service."

Keeping it in the family

Following the success of FaaS, the Bank decided to deploy the FireEye® Threat Analytics Platform (TAP) to aid in PCI DSS compliance and to provide enhanced threat detection and analysis. Peyman Gohari, Head of Security at Police Bank, described, "TAP exhibits all of the same qualities that make me a big fan of FaaS. It's great at examining event data and enabling us to rapidly determine what action needs to be taken. We can't afford to waste time: TAP integrated quickly into our environment and gave us immediate benefit. This is key for us."

One of the risk management assessments conducted by Gohari identified that incoming email traffic passing through the Bank's on-premise Exchange server could represent a potential vulnerability. Coincidentally, a phishing email supposedly from the Australian Tax Office (ATO) was the catalyst for evaluating FireEye® Email Threat Protection (ETP).

Gohari recalled, "We detected the ATO malware successfully but it took several people about six hours to fully resolve the situation. Given our experiences with FaaS and TAP we were enthusiastic to see how ETP could help. Optus came up with a proposal that was very appealing: The cost for ETP was very accessible in terms of the levels of risk remediation benefits, enabling us to quickly get approval. Implementation proved to be very straightforward too."

Klauzner added, "Because ETP dramatically reduces the volume of email carrying spam and malware, we've witnessed a commensurate decrease in bandwidth usage, enabling us to utilise our network for more productive traffic."

The Police Bank team also has implemented FireEye® Network Security (NX) to combat against Web-based cyber attacks. "The integration across our FireEye solutions is great," Gohari stated. "For example, the intelligence sharing between NX and ETP significantly strengthens our security on two of the most frequently exploited threat vectors."

Doing more with less

As with the majority of IT and IS teams, resources at Police Bank are limited, making the selection of security-related tools and solutions extremely important. "Without FaaS, to maintain a similar level of protection we would need to add at least two extra full-time heads and then still purchase additional tools," commented Klauzner.

Gohari observed, "Knowing that we have FaaS handling the really sophisticated attacks gives me the time to focus on other key areas of my job. There's always a significant amount of work to be done but FireEye gives me the extra support that I need."

"I've worked with FireEye for a long period of time," Gohari noted. "A common denominator across all of the products has been the caliber of the FireEye personnel: I've never encountered anyone that doesn't have in-depth expertise or the skills necessary to provide advice. I've worked with a lot of security companies and the FireEye people really stand out."

Klauzner summarised, "FireEye has definitely improved the overall security posture of the business, in both the visibility we now have and our ability to detect and protect.

"The sole reason for Police Bank to exist is to look after our Police Members and their extended families; we're able to do this much better with world-class protection from FireEye behind us."

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 5,300 customers across 67 countries, including more than 845 of the Forbes Global 2000.