FIREEYE™

CUSTOMER STORY

Australian Health Insurer Enhances Security Posture to Manage Risk

CBHS Health Fund Centralizes View on Security and Streamlines Alert Investigation with FireEye Solutions

CBHS HEALTH FUND

FACTS AT A GLANCE

INDUSTRY

$ Insurance

SOLUTIONS

- FireEye Endpoint Security
- FireEye Network Security
- FireEye Email Security—Cloud Edition
- FireEye Helix

BENEFITS

- Single provider for multiple threat vectors minimizes security stack complexity
- Centralized view of entire infrastructure enhances efficiency and effectiveness
- Reduction in false positives streamlines alert investigation
- Training on best practices maximizes impact of security solutions investment

CUSTOMER PROFILE

Established in 1951, CBHS Health Fund is a member-owned, not-for-profit health insurer that provides access to quality, affordable health coverage for current and former Commonwealth Bank of Australia (CBA) employees, contractors, and their families. The health fund has more than 105,000 members and provides private health insurance to over 230,000 individuals in Australia. Headquartered in Parramatta, New South Wales, CBHS has approximately 250 employees.

For CBHS Health Fund, nothing matters more than the health and happiness of its members and people. As a not-for-profit, member-owned health fund, CBHS invests all its revenue into delivering benefits to members and financing operational costs, not paying dividends to shareholders. The health fund pays out almost 93.1 cents in claims for every premium dollar received; in comparison, the industry average is 85.9 cents.

This members-first approach also informs the quality and breadth of services CBHS offers, initiatives such as The Better Living program that connects members with experts who provide coaching and support to improve health and wellbeing, and a Hospital Substitute Treatment program that tailors support to the unique health needs of individual members.

Beyond physical health, CBHS' commitment to the wellbeing of its members also entails being a responsible steward of their personal data. Joe De Battista, Chief Information Officer (CIO) at CBHS, highlighted, "The security, management, and governance of the information shared with us are absolutely paramount, as expected by our members and the regulatory framework in which we must operate. Together, cyber and information security constitute one of the material risks that our management team and Board of Directors monitor."

A well-structured governance process around risk management ensures the whole organization is committed to the risk appetite established by the Board and in accordance with industry regulation and expectation. As CIO, De Battista is responsible for implementing the controls that meet this risk appetite from a cyber security and technology perspective. The resulting security posture protects CBHS' hybrid environment, which is comprised of an on-premise and a Microsoft Azure cloud infrastructure, as well as the devices of remote and mobile workers.

In 2016, De Battista and his team set out to revitalize CBHS' cyber security capabilities and ensure defences were aligned with the organization's risk appetite. To elevate the security posture, goals were set to enhance visibility across the CBHS environment, improve the accuracy of threat detection tools and reduce complexity in the security stack.

> "The first thing we noticed after implementing the FireEye solutions was how significantly the noise dropped. The reduction in false positives freed our resources, enabling us to accomplish more proactive security tasks and better focus our efforts when we do get an alert that requires investigation."
>
> — **Joe De Battista**, , Chief Information Officer, CBHS

"There are notifications happening all the time that need to be triaged and investigated. Our previous security solutions were solid, but very noisy and generated a high rate of false positives that were very time consuming to resolve," recounted De Battista.

A Single, Industry-Leading Provider to Reduce Complexity

To align defences with the expectations established in the risk appetite statement, De Battista and his team defined an information security strategy based on key portions of the NIST security framework. When discussing opportunities to strengthen CBHS' security stack, a local partner introduced De Battista to one of its preferred technology providers: FireEye.

"The commentary on the quality and calibre of FireEye services and technology in the industry forums CBHS participates in and the CIO networking group I'm a part of really validated the credentials the company carries in the market," shared De Battista. "We implemented a Board mandate to partner with best-of-breed tier 1 providers and FireEye definitely met that requirement."

The depth and breadth of industry-leading solutions offered by FireEye addressed De Battista's objective to minimize the complexity in CBHS' security stack without compromising coverage. He explained, "Complexity is a real problem in this space: It overly burdens security teams and creates potential vulnerabilities for attackers to exploit. Convoluted controls and architecture are the last things you want to deal with in cyber security. I was very much in favour of partnering with a single tier 1 provider."

CBHS deployed FireEye Network Security, FireEye Endpoint Security, FireEye Email Security—Cloud Edition and FireEye Helix to detect and prevent threats across its infrastructure from core to perimeter. Including the time to transition out previous solutions, implementation was completed in three months.

A Centralized View on Security

FireEye Network Security identifies and stops advanced, targeted and other evasive attacks hidden in Internet traffic. By leveraging its automated workflows, the CBHS Security team can configure the solution to immediately begin investigation, validation and containment once a potential threat is detected. CBHS uses the sophisticated multi-engine architecture of FireEye Endpoint Security to provide protection for threats, as well as to launch comprehensive inspections and analyses on any attacks attempting to infiltrate the network. FireEye Email Security—Cloud Edition provides the team with the ability to rigorously inspect for, contain and neutralize email traffic weaponized against the organization.

"The first thing we noticed after implementing the FireEye solutions was how significantly the noise dropped. The dramatic reduction in false positives freed our resources, enabling us to accomplish more proactive security tasks and better focus our efforts when we do get an alert that requires investigation," remarked De Battista.

To simplify the management of defences, the CBHS security team uses the single Helix dashboard to unify security solutions across CBHS' environment and enhance their performance with next-generation SIEM, orchestration, behavioural analytics and threat intelligence.

CBHS blended self-learning and organized training from FireEye to gain a deep understanding of how best to leverage Helix to manage, search, analyse, investigate and report on the alerts generated by its security solutions. De Battista noted, "Being fully conversant with the best practices for using Helix to verify an incident, validate that appropriate action has been taken and resolve the alert on the dashboard has been very beneficial."

A Partner to Trust

The confidence De Battista and his team feel in the controls they've put in place with FireEye is essential for CBHS in meeting the Board commitment, and the expectations of members and industry regulators.

De Battista concluded, "It is critically important that I am able to report to the Board with confidence and that they can be confident that our security posture is protecting the fund to the necessary extent. We're confident in our ability to continuously evolve our controls to address a changing threat landscape and meet our Board's risk appetite. I can't overstate the value of using solutions and partnering with a provider that we trust like FireEye."

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.