CUSTOMER STORY

# Multistate Healthcare Provider

## Comprehensive protection from FireEye solutions and services

**FACTS AT A GLANCE**

**INDUSTRY**

Healthcare

**SOLUTIONS**

FireEye Network Security

FireEye Endpoint Security

FireEye Central Management

FireEye Network Forensics

FireEye Endpoint Forensics

FireEye iSIGHT

FireEye as a Service

FireEye Compromise Assessment

Mandiant Incident Response

**BENEFITS**

Integrated threat vector coverage provides seamless protection across entire infrastructure

Comprehensive threat intelligence enables proactive risk mitigation

24/7 managed detection and response from security experts to keep members' PII protected

**CUSTOMER PROFILE**

This healthcare provider has been serving employers and individuals across multiple states and its thousands of employees provide health insurance to over two million members.

In 2014, this healthcare provider experienced a cyber security incident that caused it to immediately bring in investigators from the FBI and a Mandiant incident response team. The team – comprised of Mandiant experts that specialize in tracking and blocking attacks from hackers – performed the Mandiant Compromise Assessment service to determine whether the environment had been compromised. Upon confirming evidence of a compromise, the team immediately pivoted into Incident Response to rapidly contain the attack. That fateful event began the healthcare provider's partnership with FireEye, which today has expanded to include a wide array of FireEye solutions and services.

The manager of security operations, is responsible for maintaining the integrity of members' personally identifiable information (PII). Both the manager and the incident response team are charged with protecting the company from any further external or internal threats.

"With FireEye having the proven strength of solutions, Mandiant expertise and FireEye Threat Intelligence, to me it's the clear leader in the security space"

— **manager of security operations**, healthcare provider

Each Friday, the manager of security operations briefs senior management on the latest threat intelligence landscape and provides updates on the organization's defenses. "It's all about our members' data: If we can't protect that information we'll lose our rebuilt reputation and our members' faith in us. We will not let history repeat itself. Right now, trust is a really big issue in healthcare and we're going the extra mile to safeguard our members," he noted.

**A Complete Set of Solutions and Services**

The healthcare provider has implemented a full suite of FireEye solutions that include: FireEye Network Security for detecting and blocking attacks hiding in Internet traffic; FireEye Endpoint Security protection against zero-day attacks; and FireEye Central Management to collate reporting, data sharing and threat intelligence from across the FireEye suite of solutions. "FireEye Network Security and FireEye Endpoint Security just sit there running quietly in the background and they only make noise when they find something suspicious; they're our silent partners," chuckled the manager of security operations.

The company also utilizes FireEye Network Forensics for high-speed packet capture and deep forensic analysis capability; and FireEye Endpoint Forensics to monitor and analyze activity across thousands of endpoints in real time.

**Extending Security Operations with Managed Investigation**

The healthcare provider also leverages FireEye Managed Defense; a managed detection, investigation and response service that monitors its infrastructure 24/7. The service is staffed by seasoned FireEye security professionals who employ timely, relevant threat intelligence to detect and remediate threats early in the threat lifecycle. The manager of security operations commented, "FireEye Managed Defense is an extension of my team and its experts even attend our team meetings."

The security team and the FireEye Managed Defense staff gather threat intelligence from a wide variety of sources that is forwarded to the company's security information and event management system (SIEM) to help evaluate if it is vulnerable and actions need to be taken to remediate specific threats.

**Additional Comprehensive, Integrated Threat Intelligence**

The FireEye Managed Defense experts recommended that the company leverage FireEye Threat Intelligence for timely, deeper intelligence, "We ran comparisons with other companies against FireEye Threat Intelligence," the manager of security operations recounted. "What we were looking for was the quality of the intelligence, the timeliness, and the feasibility of integrating it with the different components in our infrastructure. Threat Intelligence won the contest hands-down!"

FireEye Threat Intelligence provides proactive, comprehensive information that adds context and priority to global threats. It helps mitigate risk and bolster incident response by delivering evidence that helps to predict attacks and focus attention on the most critical issues. "FireEye Threat Intelligence is a brilliant complement to our other sources," the manager of security operations stated. "I get a wide variety of threat indicators from a single download from the FireEye Threat Intelligence portal; it puts the data into an easily-consumable format for our SIEM to quickly ingest."

FireEye

> "FireEye Helix is going to give me excellent single-pane-of-glass visibility into my entire security stack: It will free up my team to focus on incident response as well as proactive prevention throughout our company."
>
> — **manager of security operations**, healthcare provider

The manager of security operations also is impressed with the support he receives from the FireEye Threat Intelligence specialists, he observed, "They are constantly giving us information, the openness of the FireEye team is refreshing."

**Strengthening the Foundational Layer**

The manager of security operations is looking forward to purchasing FireEye Helix in the near future to provide a seamless and scalable foundation to connect and enhance all of the company's security solutions, including non-FireEye products. FireEye Helix will enable the security team to efficiently conduct essential functions, such as alert management, search, analysis, investigations, and reporting. "FireEye Helix is going to give us excellent single-pane-of-glass visibility into our entire security stack: It will free up the security team to focus on incident response as well as proactive prevention throughout the company," The manager of security operations explained.

Impressed with the comprehensive nature of FireEye solutions and services, the manager of security operations shared, "With FireEye having the proven strength of solutions, Mandiant expertise and the FireEye Threat Intelligence, to me it's the clear leader in the security space.

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 6,600 customers across 67 countries, including more than 45 percent of the Forbes Global 2000.

FireEye®