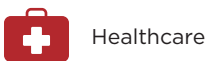




Pharmaceutical Benefits Management Company Raises the Bar on Security

FACTS AT A GLANCE

INDUSTRY



Healthcare

SOLUTIONS

FireEye Network Security

FireEye Endpoint Security

FireEye Central Management

Mandiant Incident Response services

BENEFITS

Immediate insight to endpoint activity and its full scope of impact

Detection and blocking of zero-day threats leveraging global threat intelligence

Instant support in the event of a breach

Significant improvement in the quality of triage and speed of investigation

CUSTOMER PROFILE

This pharmaceutical benefits management company services healthcare plans provided by employers and third-party administrators. The company supports millions of members, delivering services that include pharmacy network management, benefit administration, claims processing, marketing support, report building, and formulary design.



This pharmaceutical benefits management company holds a great deal of medical information about its clients, from prescription drug purchases to medical histories. Information security is crucial, especially as the company must comply with several regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS).

Seeking Answers

With its infrastructure spanning over five thousand IT endpoints and multiple data centers, the incident response manager admitted, "We wanted more immediate endpoint visibility to increase our ability to instantly detect an incident and have the right tools to optimally mitigate the risk associated with it."

The company had experienced identifying potentially suspicious network traffic but the legacy tools lacked the ability to determine if the circumstances were malicious, or simply caused by misconfiguration or other innocuous circumstances. The incident response manager recounted, "I consulted with several of our incumbent vendors and received the suggestion that we install FireEye Network Security to inspect the traffic and monitor any alerts that were raised."

“We appreciate the very low false-positive rate for which both FireEye Network Security and FireEye Endpoint Security are known; FireEye solutions have enabled us to take our incident response to a level far above that of a year ago.”

— Incident Response Manager, pharmaceutical benefits management company

Initial Experience with FireEye

The company agreed that deploying FireEye Network Security would be a prudent investment. “The solution was very easy to set up,” recalled the incident response manager, “it was up and running in a few hours.”

For the security team, the performance of FireEye Network Security underscored the advantages of behavior-based FireEye detection capabilities. Located at infrastructure’s egress points, the solution inspects both incoming and outgoing traffic. “It was almost as if we lifted up a rock looking for one thing – like targeted phishing, which luckily we didn’t find – but uncovered concerning items in-house that our legacy, signature-based tools had not discovered,” the incident response manager shared.

An additional benefit of FireEye Network Security is the FireEye Dynamic Threat Intelligence cloud: By having access to globally-shared intelligence obtained from FireEye customers worldwide, FireEye Network Security screens for and detects zero-day threats.

Detailed Endpoint Data

With the success of the network solution, the company installed FireEye Endpoint Security as a proof-of-concept to provide visibility into any user’s behavior on a PC prior to it being potentially infected. “It not only facilitates forward tracking in a ‘kill chain’ to pinpoint where the phishing link was clicked, and what was downloaded, but also it enables us to go backwards and trace the emails, find out who else has received them, and really identify the scope and potential severity of an attack,” enthused the incident response manager.

The data obtained from FireEye Endpoint Security during the trial period was so valuable, the company immediately

rolled it into a company-wide deployment. “While we initially had Endpoint Security in place just to find the malicious code that people were downloading from the Internet, it also gives us the ability to remotely contain a device if we think that something truly malicious is taking place and prevent the threat from spreading,” noted the incident response manager.

Boosting Incident Response

After working closely with FireEye staff and being impressed with the caliber of expertise, the company contracted the FireEye Mandiant Incident Response service to support the security team if a breach should occur. “The FireEye Mandiant consultants are leading-edge security specialists,” the incident response manager remarked. “Every one of our interactions – including the onsite training – has been a great experience.”

Moving the Bar Much Higher

To keep the team’s efficiency at peak levels, the company implemented FireEye Central Management to centralize, collate and share all data from its FireEye solutions through a single user interface. The security team can swiftly drill down and receive the detail it needs to respond to an alert. “Being able to open the incident package and immediately analyze exactly what happened is immensely powerful,” the incident response manager commented.

He continued, “We appreciate the very low false-positive rate for which the FireEye solutions are known; they have enabled us to take our incident response to a level far above that of a year ago. Our visibility into the endpoints on the network is transformed: Not only are we detecting and addressing incidents far more quickly but the quality of that triage and investigation has significantly improved.”

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

© 2018 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. CS.PBMC.US-EN-082018

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.

