CUSTOMER STORY

Biopharmaceutical Innovator Accelerates Threat Detection and Response

Hutchison MediPharma Protects Global Assets with FireEye

Hutchison Medi Pharma

FACTS AT A GLANCE

INDUSTRY

Healthcare

SOLUTIONS

- FireEye Network Security
- FireEye Endpoint Security
- FireEye Central Management

BENEFITS

- Centralized, streamlined analysis of threats has significantly improved incident response time
- Multi-vector traffic analysis provides early threat detection
- Real-time exchange of threat intelligence rapidly fortifies defenses during attacks

CUSTOMER PROFILE

Hutchison MediPharma (HMP) was founded in 2002 to oversee research and development of drug candidates for the holistic treatment of cancer and immunological diseases. The company is part of Hutchison China MediTech Limited (Chi-Med) and has a scientific team of nearly 500 people spread across locations in both China and the US.

Committed to addressing the unmet needs of patients, Hutchison MediPharma (HMP) is developing novel drug candidates with the potential for best-in-class efficacy. The company's global leadership in the discovery, research and development of targeted therapies has led to partnerships with other renowned innovators in biopharmaceutics, including AstraZeneca and Eli Lilly.

HMP's operations—from chemistry, biology, pharmacology and toxicology processes to manufacturing, clinical and regulatory functions—are all integrated across a multinational infrastructure. A key facet of HMP's success has been maintaining a stable, controlled environment for the hundreds of scientists and clinicians who rely on this ecosystem to develop treatments. Cyber security plays a central role in this effort.

Pharmaceutical companies, particularly those engaged in research and development, attach great importance to information security. Creating new medical treatments is a long, arduous process, but it is the defining purpose for these organizations. Protecting this intellectual property is a business imperative.

HMP's head of IT security and infrastructure, Jonathan Shi, emphasized the necessity of securing this mission-critical information, "A cyber attack could have devastating consequences, not only for the confidentiality of HMP's drug formulas but also the personal information we've pledged to protect on behalf of patients, employees and stakeholders. In addition to the impact at a personal level, a breach could inflict significant reputational and financial damage."

Though HMP's legacy security stack had reliably defended the company's assets for years, the amount of time required to interpret the incoming alerts and manage the individual products eventually became unsustainable for the IT security team. The defenses also lacked deep visibility into HMP's distributed environment. By enhancing the quality of

> "With FireEye's help we've significantly improved HMP's incident response time and now can efficiently analyze threats and determine their root causes."
>
> — **Jonathan Shi**, Head of IT Security and Infrastructure

this threat intelligence, Shi saw an opportunity to simultaneously improve HMP's threat detection and analysis capabilities and better equip his team for efficient incident response.

Minimal Intervention for Maximum Protection

To identify a cyber security provider with a comprehensive set of solutions best fitted to its needs, HMP turned to Gartner's Magic Quadrant for Security Information, which brought FireEye to Shi's attention. With help from FireEye engineers, HMP coordinated a multi-month proof of concept (POC) to validate the effectiveness of FireEye's security methodology. The tested solutions—FireEye Network Security, FireEye Endpoint Security and FireEye Central Management—excelled.

The solutions' capacity for thorough traffic monitoring and early threat detection were critical aspects of the POC evaluation. "We were impressed when FireEye Network Security efficiently identified a client behaving suspiciously and generating abnormal traffic. In real time, FireEye Central Management exchanged intelligence on the threat with all the FireEye Endpoint Security agents. With minimal intervention from our team, HMP's entire environment was fortified against the malware," recalled Shi.

Over the next two months, HMP partnered closely with FireEye to deploy the solutions across its network, servers, storage repositories and hundreds of endpoints.

Intuitive and Efficient Incident Response

Endpoint Security enables vigilant oversight of all the clients connected to HMP's network. Shi explained, "Our perimeter security is much more effective with FireEye Endpoint Security. The solution excels at discovering threats and preventing attacks before they can gain a foothold in our environment." FireEye Endpoint Security automatically isolates compromised devices for forensic analysis and remediation before deploying updated protections to all the other agents.

Advanced malware analysis engines equip both FireEye Endpoint Security and FireEye Network Security with the ability of rapid detection of known and unknown threats. The latter also incorporates the latest actionable machine, attacker and victim intelligence from the frontlines to facilitate efficient analysis and resolution of security incidents. Shi enthused, "This enhanced visibility has greatly improved HMP's network information security by giving us defenses capable of detecting and stopping attacks as they begin to emerge."

A unified security dashboard, FireEye Central Management correlates data across HMP's security systems. "The coordination by Central Management makes threat resolution across our FireEye deployment even faster," noted Shi.

In addition to improving the operational efficiency of defenses, FireEye Central Management regularly exchanges dynamic threat intelligence to ensure comprehensive, adaptive protection across all of HMP's threat vectors. Shi remarked, "Instead of requiring IT staff to assess alerts one-by-one in isolation, the platform synthesizes multiple data feeds to intuitively present details on an attack's lifecycle, path and corresponding threat level. With FireEye's help we've significantly improved HMP's incident response time and now can efficiently analyze threats and determine their root causes."

A Partner for Tomorrow's Defenses

Reflecting on the impetus to future-proof HMP's defenses, Shi concluded, "Cyber threats will continue to become increasingly complex and sophisticated. We'll witness highly intelligent attacks from all directions, including mobile, IoT and cloud vectors. Constantly mastering new defense techniques and knowledge, and then assimilating these into HMP's security posture is a must. FireEye has been an exceptional partner in helping HMP fundamentally improve our defenses."

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™