



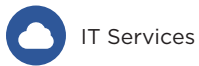
CUSTOMER STORY

CyberSecurity Malaysia



FACTS AT A GLANCE

INDUSTRY



IT Services



In pursuit of Its charter, CyberSecurity Malaysia has left no stone unturned.

The national cybersecurity agency housed under Malaysia's Ministry of Science, Technology and Innovation (MOSTI), CyberSecurity Malaysia has its sights set on becoming a globally recognized reference for national cyber security and a model for the Asia Pacific region. It's well on its way with nearly a dozen services catering to the needs of public sector, private sector and Internet users, including:

- **Cyber999:** Emergency response expertise available to help the Malaysian public detect, interpret and respond to computer security incidents such as cyber harassment, malware and targeted attacks.
- **CyberCSI:** Full-spectrum digital forensic services, training and certifications, as well as data recovery, data sanitization and litigation services for government and law-enforcement agencies and private organizations.
- **CyberDEF:** Threat detection, threat eradication and forensic analysis dedicated to securing critical national cyber security infrastructures.

“FireEye tools and services are readily incorporated into our CyberDEF program and related security best practices.”

— **Dr. Aswami Fadillah Mohd Ariffin**, Vice President, Cyber Security Responsive Services Division, CyberSecurity Malaysia

The latest threats in southeast asia

Serious cyber attacks are not rare in Southeast Asia. According to Southeast Asia: Cyber Threat Landscape¹, about 29% of FireEye customers in the region—almost 10% more than the global average—have detected malware associated with advanced persistent threat (APT) attack groups. These groups, comprised of the most sophisticated cyber attackers, are often well-funded and sponsored by nation states. Nearly 25% of their malware targets government organizations. The most targeted industries, at a collective 35%, are entertainment, media and hospitality. Given the government backing of most APT groups, this is not surprising. Government and media organizations are logical targets for intelligence gathering, vandalism and subversion.

The mission of CyberSecurity Malaysia includes protection against these latest threats, incident response for APT group-sourced breaches and forensic investigation in the aftermath of advanced attacks.

A model for cyber security expertise

Because threats and attackers have become more sophisticated, the applied research branch of CyberSecurity Malaysia has sought out the best off-the-shelf tools and expertise from around the globe. While CyberSecurity Malaysia develops most of its tools and practices in house, it strives to integrate all quality sources of intelligence and technology into its security solutions and processes. These customized solutions are necessary to deal with the unique challenges, needs and threats faced by its Malaysian stakeholders and clients.

As evidenced by Cyber999, CyberCSI and CyberDEF, CyberSecurity Malaysia serves a wide expanse of customers. Law enforcement groups gain the benefit of their technical services. Critical infrastructure organizations gain essential cyber security services. And everyone from corporate to government to individual users can use CyberSecurity Malaysia training and outreach programs.

The FireEye contribution

To identify companies that could make a strong contribution to its security foundation, CyberSecurity Malaysia researched providers based on recognition of brand and established quality, independent investigation and due diligence based on testing and testimonials. FireEye was one such company, with its Network Security (NX Series) and Central Management (CM Series) products clearing the rigors of the simulated environment CyberSecurity Malaysia developed to evaluate security technologies. Primarily applied to the CyberDEF program, FireEye technologies passed the first phase of trials and have since been considered ready for deployment in real-world scenarios.

The appeal of the Network Security products was driven by the NX sensor, which helps detect malware and botnet infections. Combined with Central Management products, CyberSecurity Malaysia is able to generate regular reports containing high-value indicators of compromise based on validated alerts. These reports help guide remediation efforts.

High-value cyber security

When its security systems generate alerts, CyberSecurity Malaysia analyzes and investigates those alerts and uncovers root causes and false positives manually. FireEye products have increased the efficiency of security processes for CyberSecurity Malaysia, including minimizing wasteful alerts—specifically, false positives.

To gain more context for these alerts and further reduce manual labor, CyberSecurity Malaysia is exploring the possibility of FireEye Advanced Threat Intelligence. The agency also continues to supplement its expertise with the latest FireEye cyber security training on alert comprehension and remediation practices to learn how to more effectively analyze malware caught by FireEye technologies.

“Overall, we were quite impressed with the high-value alerts produced by FireEye.”

— **Dr. Zahri Yunos**, Chief Operating Officer, CyberSecurity Malaysia

The impact of support and services

To provide support for local customers, FireEye maintains offices in both Singapore and Malaysia. As part of its evaluation process, CyberSecurity Malaysia accessed these support services and rated them excellent. They were a key factor in the decision to adopt FireEye products as a cyber threat mitigation solution.

Recognition and awards

Based on the quality of its cyber security approach, processes and practices, and its integration of FireEye technologies, CyberSecurity Malaysia recently received the 2015 FireEye Customer Award for Best Cyber Security Innovation. This award recognizes companies that have shown sterling initiative and ingenuity in adopting FireEye technology, expertise and intelligence into their own offerings. Continuing on its path, CyberSecurity Malaysia will likely not only realize its aspirations to become a world-class cyber security organization but also become a globally-recognized reference for cyber security in the Asia Pacific region.

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

©2019 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-EXT-CS-US-EN-000140-01

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.

